

Simplifying Cyber Security since 2016

HACKERCOOL

September 2024 Edition 7 Issue 9 Learn how Black Hat Hackers hack

Hacking with Quasar RAT

in
HACKING TOOL

VULNERABILITY FOR BEGINNERS

SolarWinds Web HelpDesk CVE-2024-28987

WHAT's NEW

Kali Linux 2024.3

VULNERABILITY FOR BEGINNERS

SonicWall Firewall CVE-2024-40766

Copyright © 2024 Hackercool CyberSecurity (OPC) Pvt Ltd

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to the publisher, addressed "Attention: Permissions Coordinator," at the address below.

Any references to historical events, real people, or real places are used fictitiously. Names, characters, and places are products of the author's imagination.

Hackercool Cybersecurity (OPC) Pvt Ltd.
Banjara Hills, Hyderabad 500034
Telangana, India.

Website :
www.hackercoolmagazine.com

Email Address :
admin@hackercoolmagazine.com



HACKERCOOL

Simplifying Cybersecurity

Information provided in this Magazine is strictly for educational purpose only.

Please don't misuse this knowledge to hack into devices or networks without taking permission. The Magazine will not take any responsibility for misuse of this information.

Then you will know the truth and the truth will set you free.
John 8:32

Editor's Note

Edition 7 Issue 9

8

"ACTIVE DIRECTORY HAS BEEN AN ADVERSARY'S FAVOURITE TARGET FOR DECADES. IDENTITY ATTACK PATHS IN AD LET MALICIOUS ACTORS MOVE Laterally AND ESCALATE PRIVILEGE IN WAYS THAT ARE EXTREMELY DIFFICULT FOR DEFENDERS TO DETECT."

-ANDY ROBBINS, PRINCIPAL PRODUCT ARCHITECT AT SPECTEROPS AND CO-CREATOR OF BLOODHOUND

INSIDE

See what our Hackercool Magazine's September 2024 Issue has in store for you.

1. Vulnerability for beginners:

[SolarWinds Web Helpdesk CVE-2024-28987.](#)

2. Hacking Tool:

[Quasar RAT.](#)

3. What's New:

[Kali Linux 2024.3](#)

4. Cyber Security:

[CrowdStrike: the massive companies you have never heard of with a hidden grip on our lives.](#)

5. Vulnerability for beginners:

[SonicWall Firewall CVE-2024-40766](#)

6. Online Security:

[Exploding pagers and walkie-talkies are a reminder of how easily your devices can be hacked - here's how to make sure they are safe.](#)

Downloads

Other Useful Resources

SolarWinds Web HelpDesk vulnerability

VULNERABILITY FOR BEGINNERS

In the first Vulnerability for beginner's article of this month's Issue, you will learn everything about a vulnerability in SolarWinds Web Help Desk (WHD) Software. Solar Winds Web Help Desk is a free help desk ticketing system software made by SolarWinds. This is used to manage service tickets by tracking their lifecycle from ticket creation to resolution. It is a web-based interface available for Windows, Linux and Mac. It is estimated that SolarWinds IT management products are used by over 3,00,000 customers worldwide.



DID YOU KNOW?

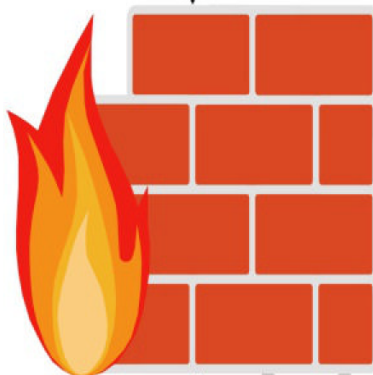
*Very soon you can checkout with
all type of cards to subscribe to*

Hackercool

Magazine

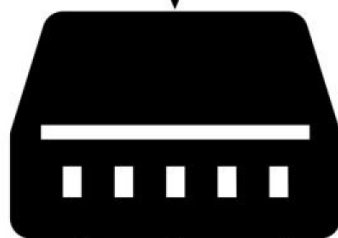


Network gateway



Firewall

Hackercool Magazine



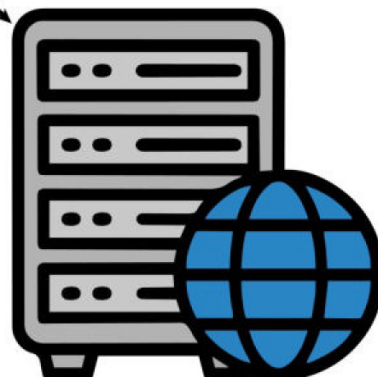
Network Switch



Customer Service agent



Customer Service agent

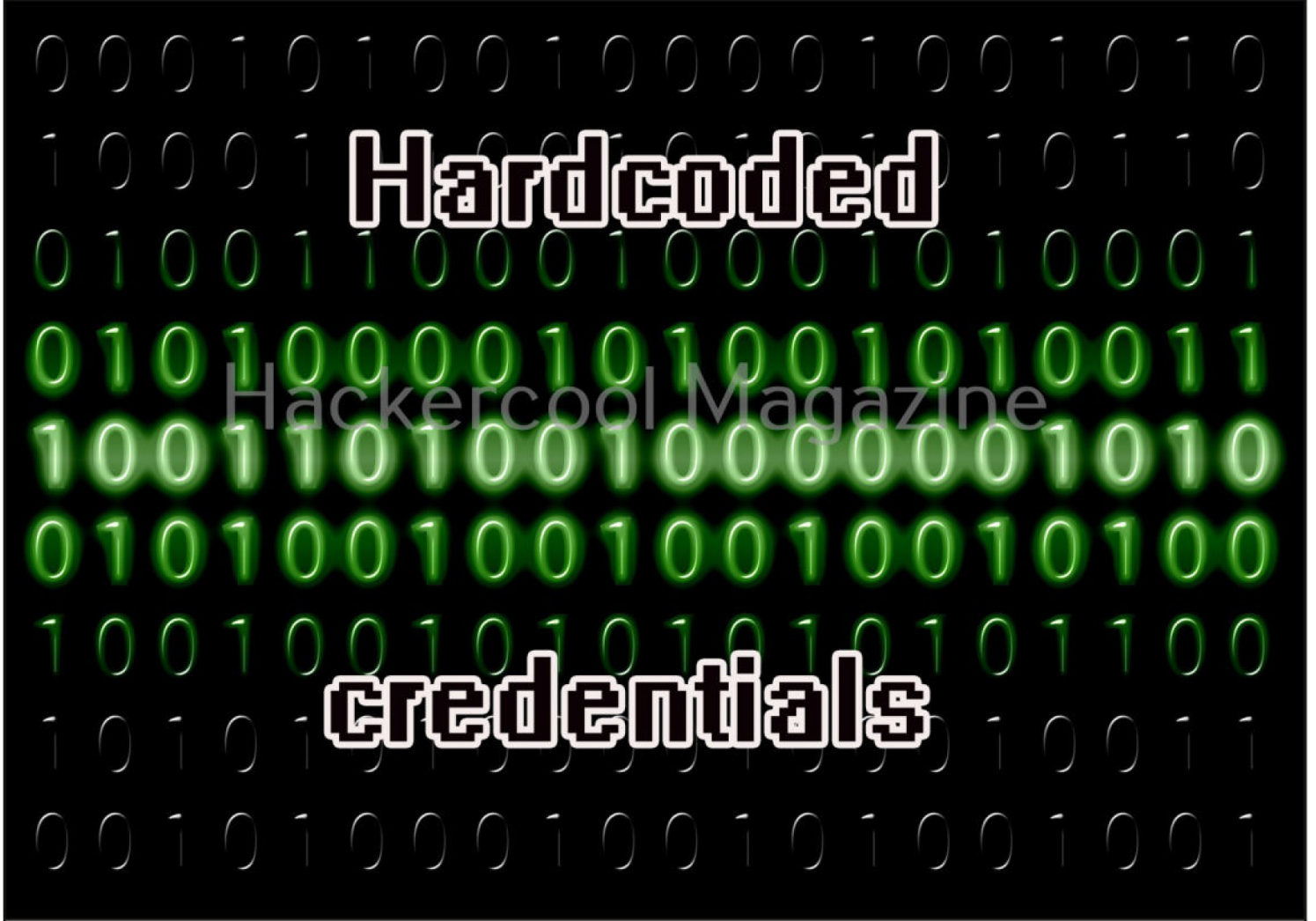


SolarWinds Web HelpDesk server

What is the vulnerability?

The vulnerability, being tracked as CVE-2024-28987 is a hardcoded credential vulnerability that can allow unauthenticated attackers to read and modify all ticket details on the server and that too remotely.

Hardcoded credential vulnerability occurs when credentials such as usernames and passwords are embedded in the source code of an application or script.



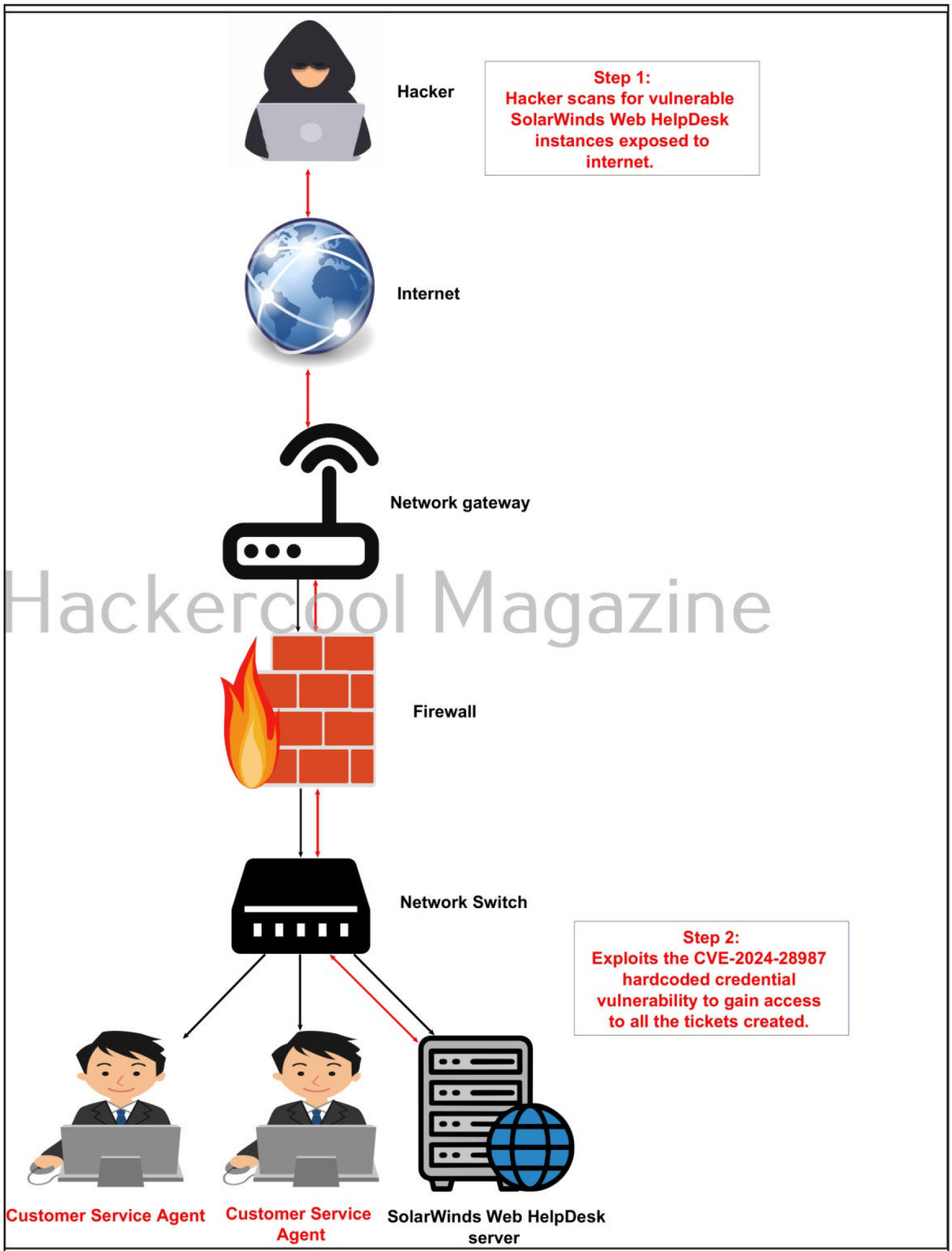
Hardcoded

credentials

How this vulnerability can be exploited?

This vulnerability can be exploited on SolarWinds Web Help Desk installed if they are exposed to the internet or the hackers already has gained access to other devices on to network.

CISA added this SolarWinds Web HelpDesk vulnerability (CVE-2024-28987) to its exploited vulnerabilities catalog on October 16 2024. CISA however did not disclose which threat actor exploited this particular vulnerability.



Impact

Horizon.ai who identified this vulnerability found over 827 instances of SolarWinds Web Help Desk reachable from internet. Majority of these instances are found in USA, France, Canada, China, India. Although exploiting this vulnerability doesn't give hackers complete access to the Web Help Desk server, it can expose data of all the tickets on that server. These tickets can contain sensitive information related to password reset, user onboarding etc.

Exploiting this vulnerability can also lead to lateral movement on the target network.

What to do to protect yourselves?

As soon as the vulnerability was disclosed, SolarWinds already released patches to the vulnerability. Your Web Help Desk software needs to be updated to versions 12.8.7 Hotfix 2. The company has provided details on how to apply the hotfix here. Also, it is a good practice to restrict internet access to the Web Help Desk server if it is not required or not in use.

Quasar RAT

HACKING TOOL

During penetration testing, after gaining initial access, pen testers use a payload to interact with the target system. There are two types of payloads pen testers often use. The first one is a through a command line shell like Meterpreter and another one is a graphical option like Remote Administration Tools (RATs). In this month's Issue, you will learn about a RAT that is still used by Black Hat hackers and Red Teamers around the world. It's called Quasar RAT.

Quasar RAT is an open-source RAT for Windows that is very fast and light weight. The tool coded in C# has features like,

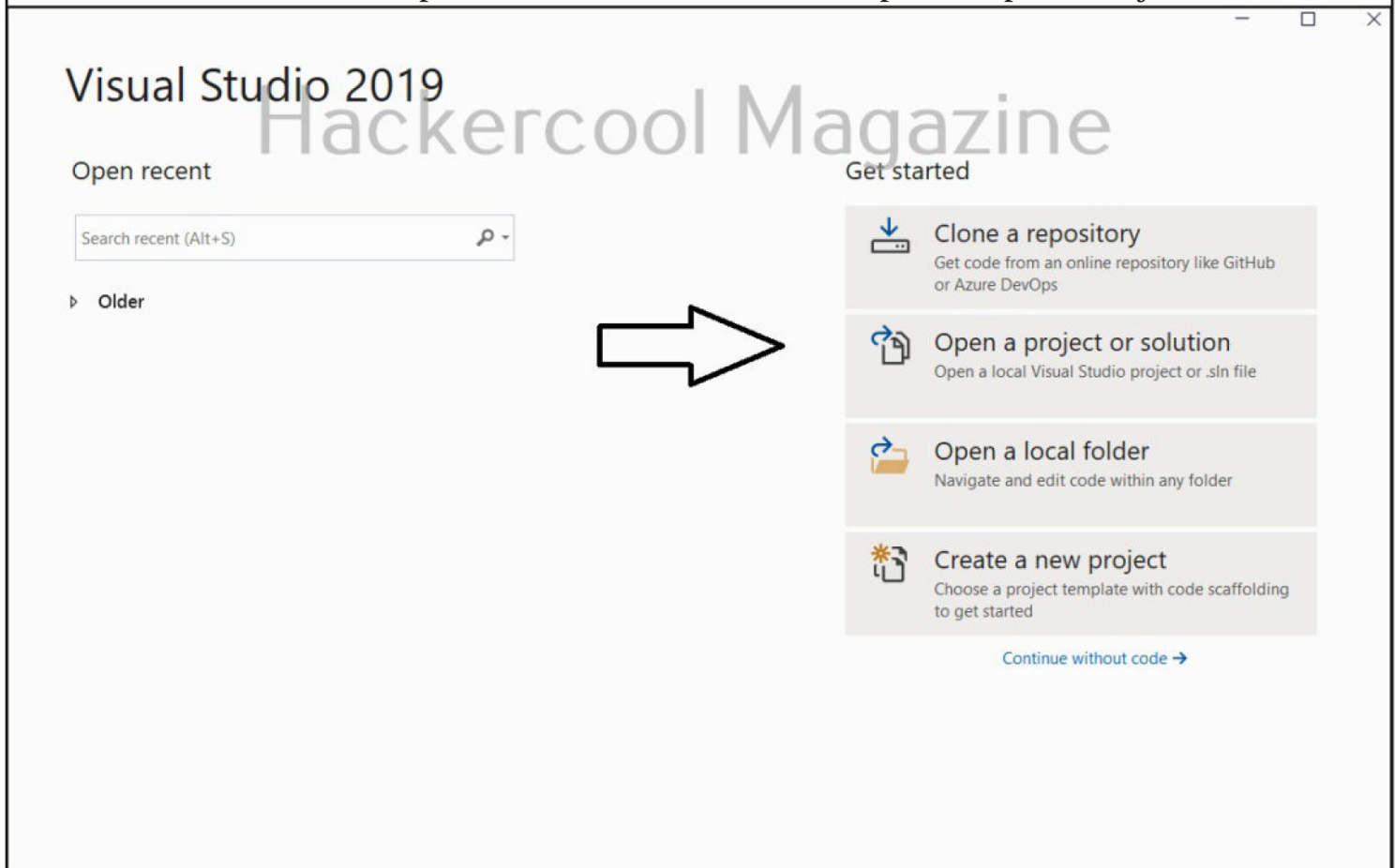
- 1) Viewing system information of the target system
- 2) Keylogger
- 3) Remote shell
- 4) Remote file execution
- 5) TCP network streaming
- 6) Fast network serialization
- 7) Encrypted communication using TLS
- 8) UPnP support for automatic port forwarding
- 9) Task manager
- 10) File manager
- 11) Startup manager
- 12) Remote Desktop
- 13) Registry editor
- 14) System Power commands
- 15) Reverse proxy
- 16) Password recovery from browsers and FTP clients.

Quasar RAT supports any Window machine starting from Windows 7 to Windows 11 and Windows Server 2008 R2 to Windows Server 2022. It requires .NET Framework 4.52 or higher to run.

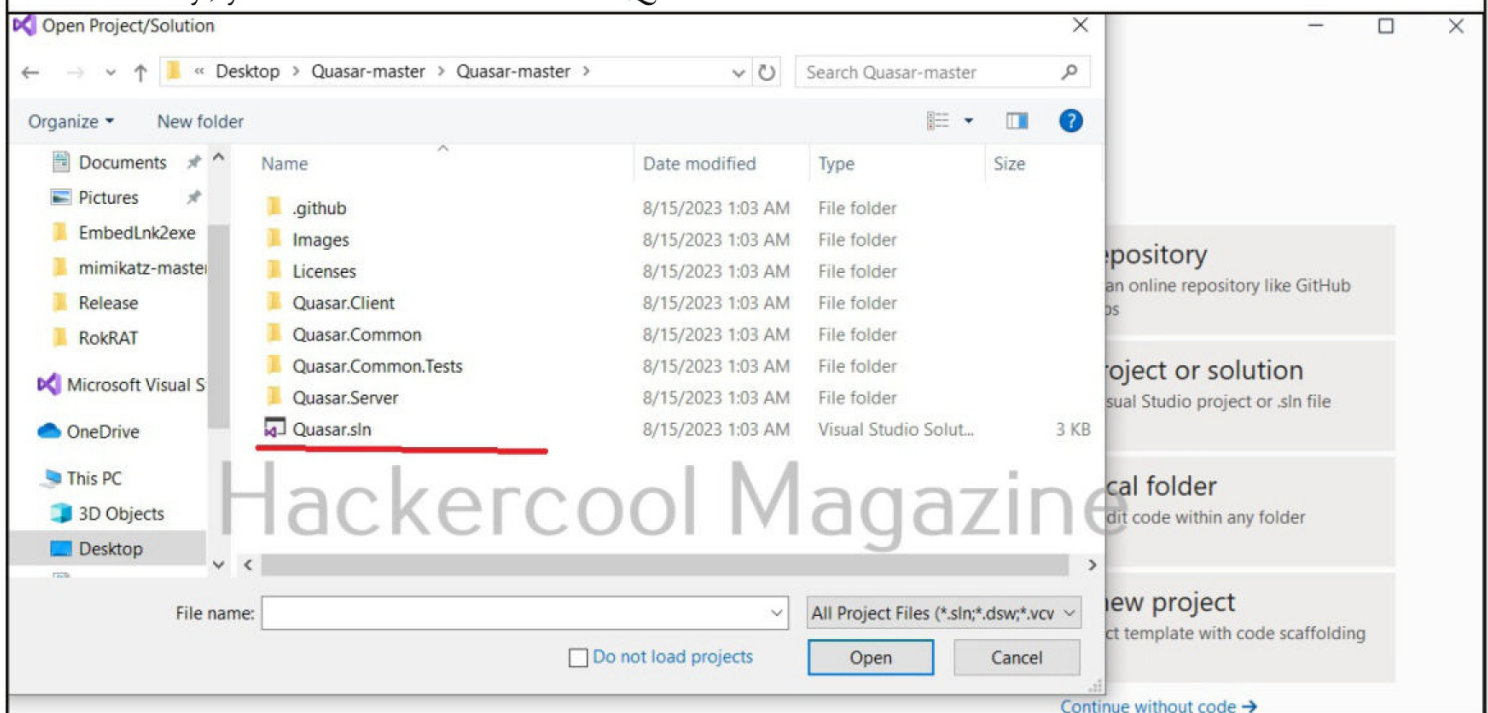
Let's show you how to compile this tool. The download information of Quasar RAT is given in

our Downloads section. For this tutorial, we are using Windows 10 with Visual Studio installed. As it is a CSHARP project, it needs visual studio to compile the code. Make sure the version of Visual Studio is > 2019+.

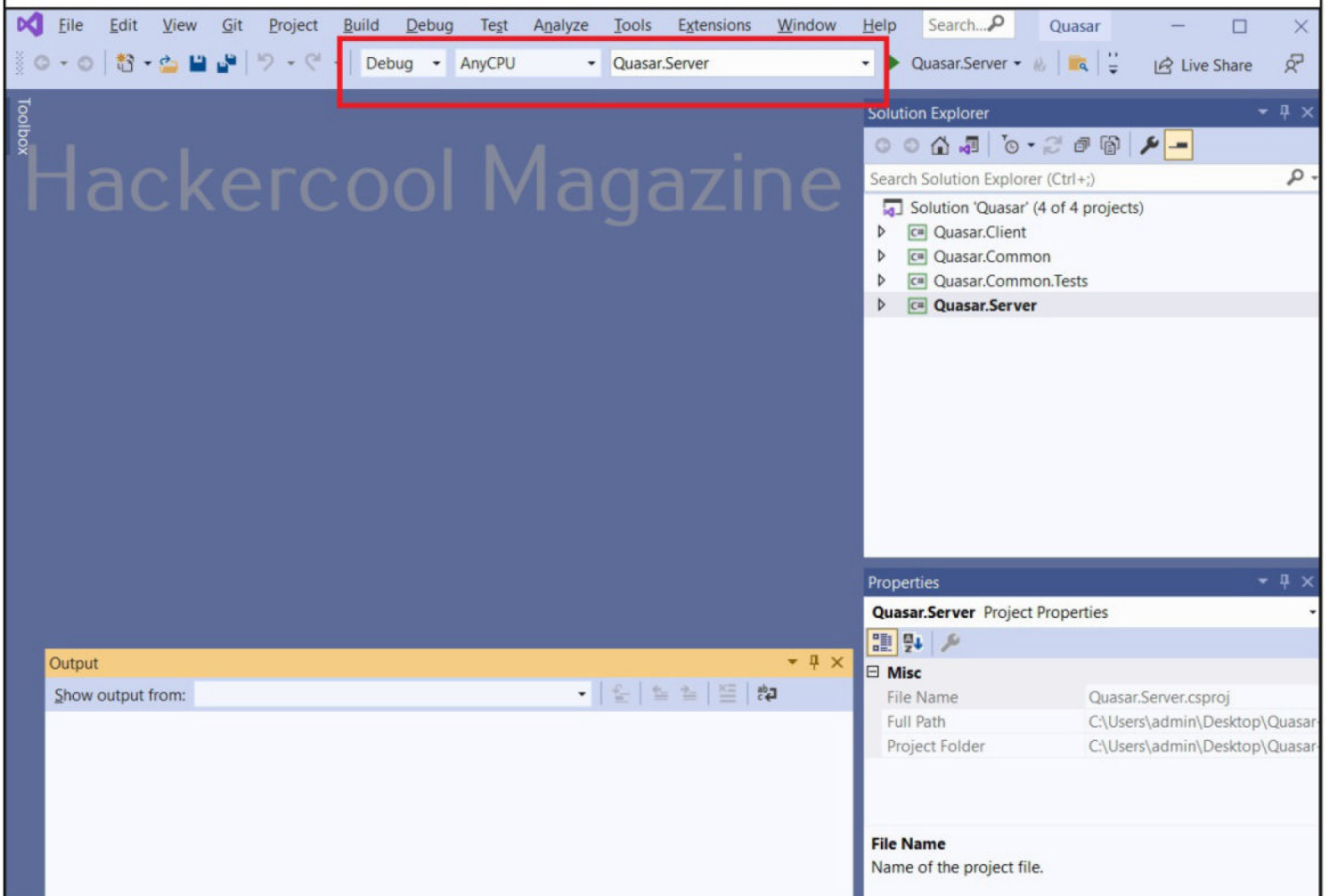
Extract the contents of the zip archive downloaded. After extracting the content of the zip archive downloaded to a folder, I open Visual Studio and click on option "Open a Project or solution".



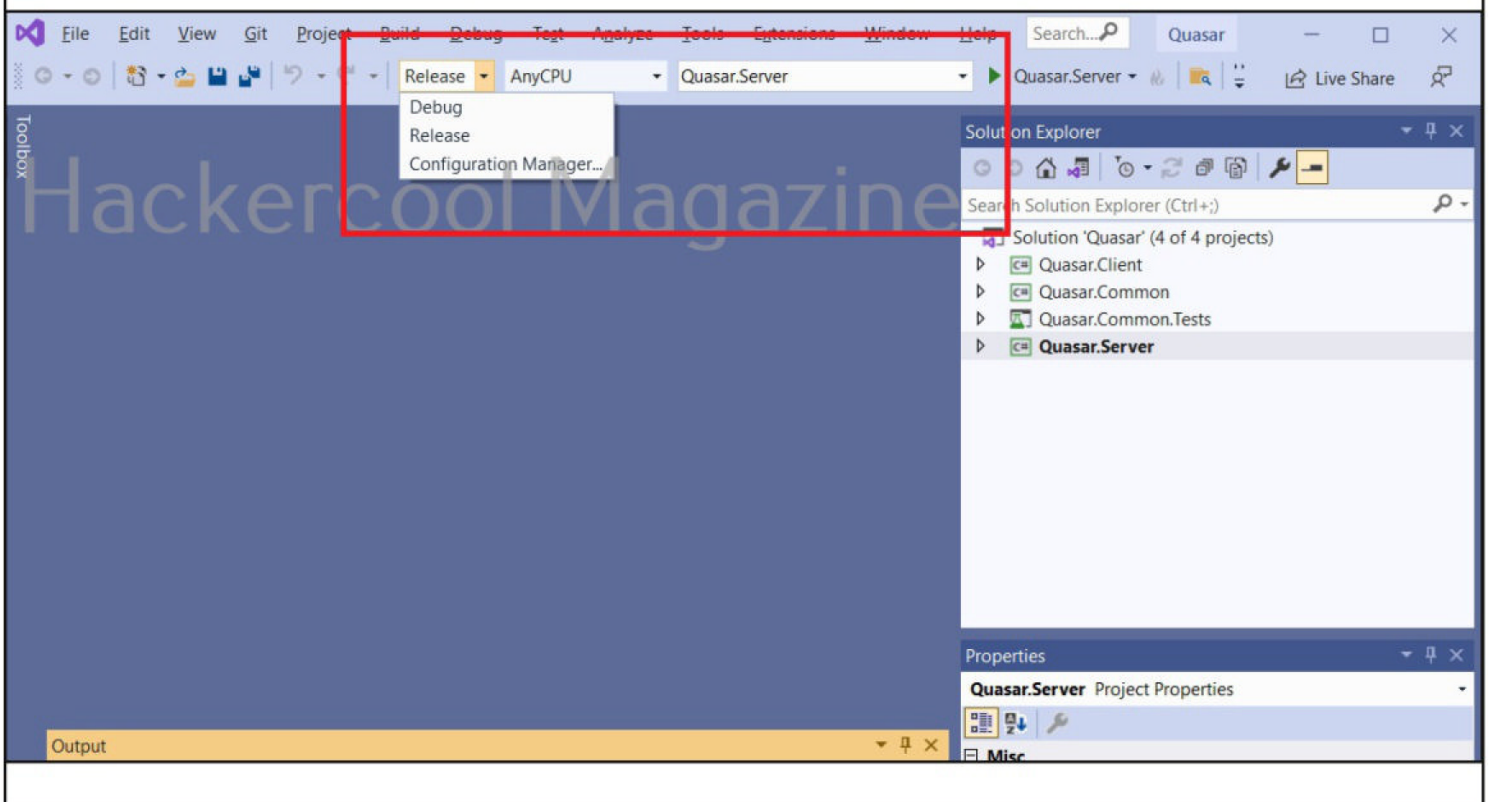
Navigate to the directory where the extracted contents of the Quasar Zip archive are located. In that directory, you will find a file named Quasar.stn as shown below.

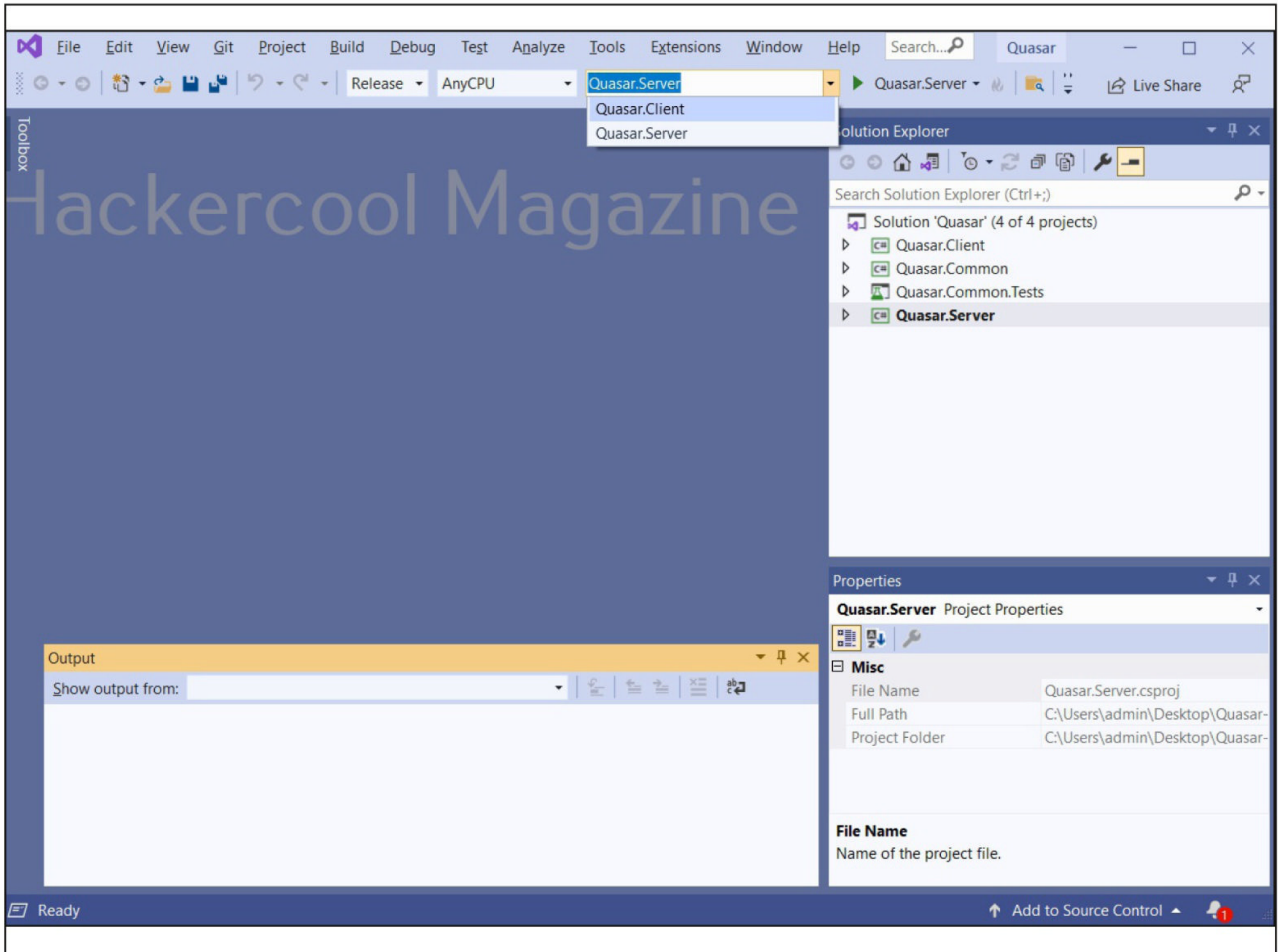


Click on it. The solution will be loaded into Visual Studio.

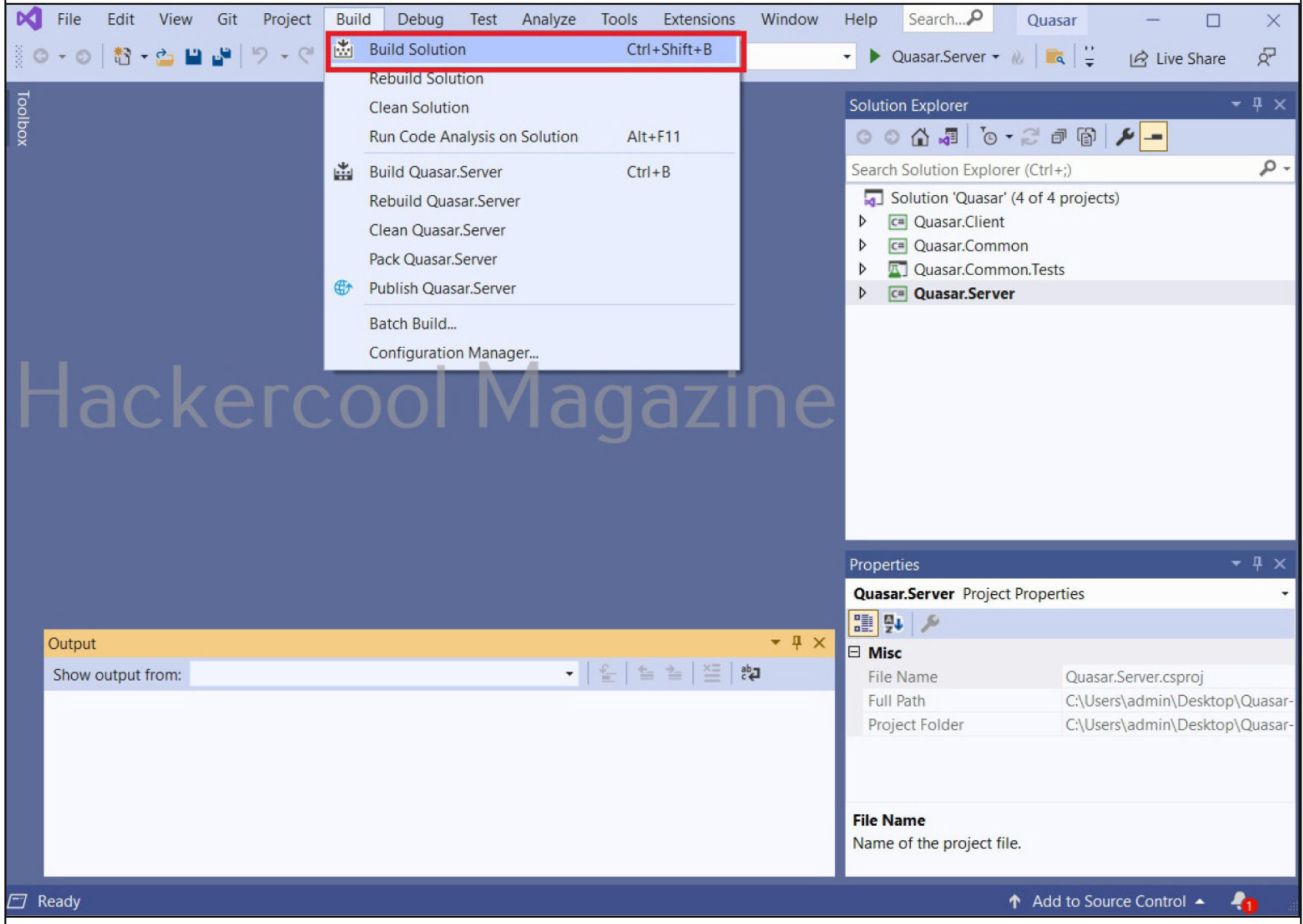


In the highlighted part above, select release and select 'Quasar Server'.





From the build menu, select “Build solution or just use shortcut “Ctrl+shift+B” to compile the solution.



In the output section, check the status of the compilation to see if it is successful or not.

The screenshot shows the Visual Studio IDE with the following components:

- Menu Bar:** File, Edit, View, Git, Project, Build, Debug, Test, Analyze, Tools, Extensions, Window, Help.
- Toolbar:** Includes icons for undo, redo, save, and other standard IDE functions. The build configuration is set to Release, AnyCPU, and the project is Quasar.Server.
- Solution Explorer:** Displays the solution 'Quasar' (4 of 4 projects):
 - Quasar.Client
 - Quasar.Common
 - Quasar.Common.Tests
 - Quasar.Server** (selected)
- Properties Window:** Shows the Project Properties for Quasar.Server. The Misc section is expanded, showing:

Property	Value
File Name	Quasar.Server.csproj
Full Path	C:\Users\admin\Desktop\Quasar-master\bin\Release\net452\Bo
Project Folder	C:\Users\admin\Desktop\Quasar-
- Output Window:** Shows the build output for the Build configuration:


```

3>Added assembly 'C:\Users\admin\Desktop\Quasar-master\Quasar-master\bin\Release\net452\Qu
3>Added assembly 'C:\Users\admin\Desktop\Quasar-master\Quasar-master\bin\Release\net452\Bo
3>Merging 5 assemblies to 'C:\Users\admin\Desktop\Quasar-master\Quasar-master\bin\Release\n
3>Merge succeeded in 4.6760242 s
3>      1 file(s) copied.
3>Done building project "Quasar.Client.csproj".
===== Build: 4 succeeded, 0 failed, 0 up-to-date, 0 skipped =====
      
```
- Status Bar:** Shows "Build succeeded" and "Add to Source Control" button.

Similarly compile the client too.

The screenshot shows the Visual Studio IDE with the following components:

- Menu Bar:** File, Edit, View, Git, Project, Build, Debug, Test, Analyze, Tools, Extensions, Window, Help.
- Toolbar:** Includes icons for Build, Run, and other development actions. The Build dropdown is set to 'Release' and the CPU architecture is 'AnyCPU'. The active project is 'Quasar.Client'.
- Solution Explorer:** Displays the solution 'Quasar' containing four projects: Quasar.Client, Quasar.Common, Quasar.Common.Tests, and Quasar.Server.
- Output Window:** Shows the build output for the 'Build' configuration. The log indicates that the build for Quasar.Server succeeded.
- Properties Window:** Displays the 'Misc' properties for the 'Quasar.Server' project, including the file name, full path, and project folder.

Output Window Log:

```

Build started...
1>----- Build started: Project: Quasar.Server, Configuration: Release Any CPU -----
1>Quasar.Server -> C:\Users\admin\Desktop\Quasar-master\Quasar-master\bin\Release\net452\Q
===== Build: 1 succeeded, 0 failed, 3 up-to-date, 0 skipped =====
  
```

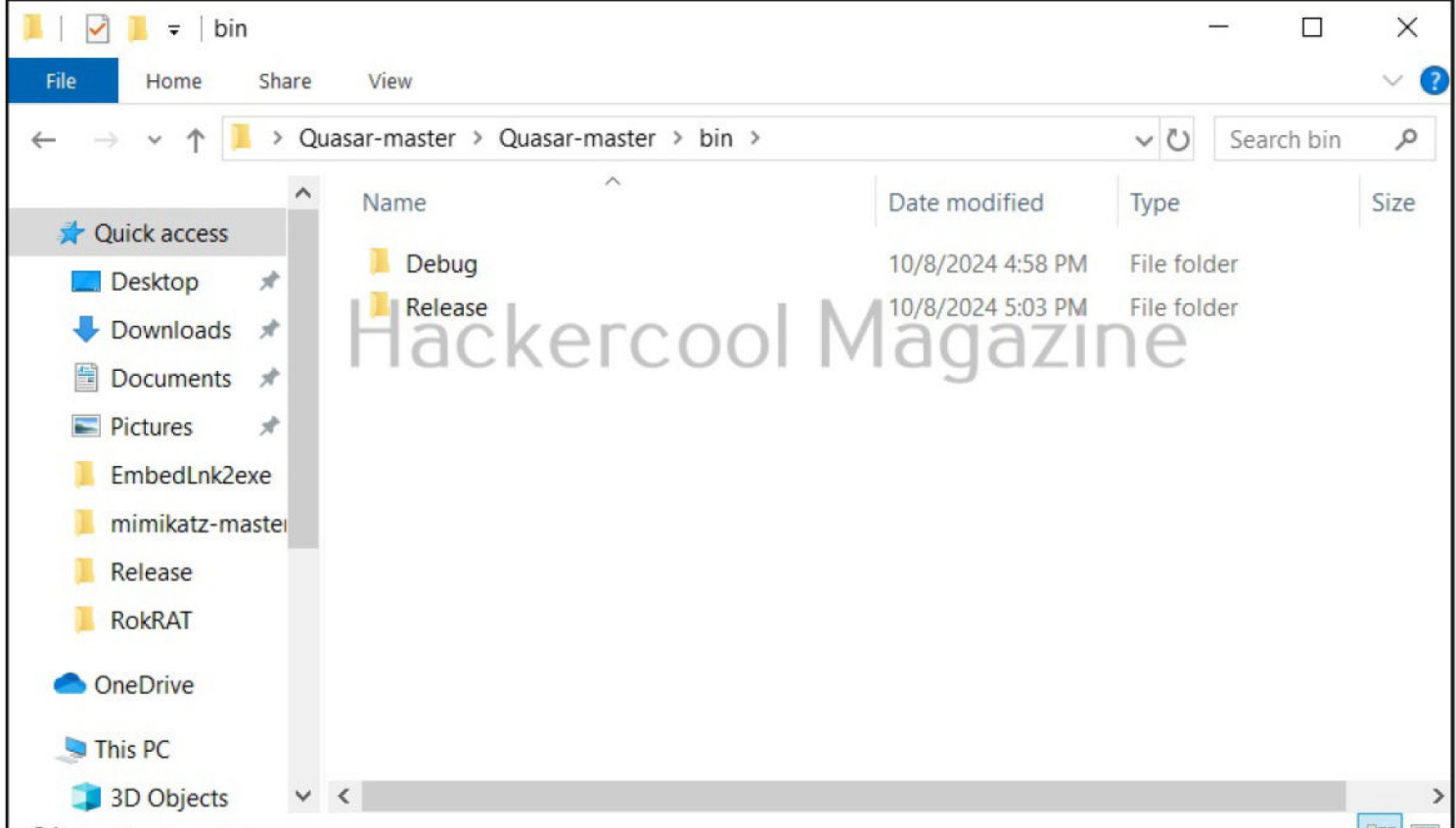
Properties Window (Quasar.Server Project Properties):

Misc	
File Name	Quasar.Server.csproj
Full Path	C:\Users\admin\Desktop\Quasar-master\Quasar-master\bin\Release\net452\Q
Project Folder	C:\Users\admin\Desktop\Quasar-master\Quasar-master\bin\Release\net452\Q

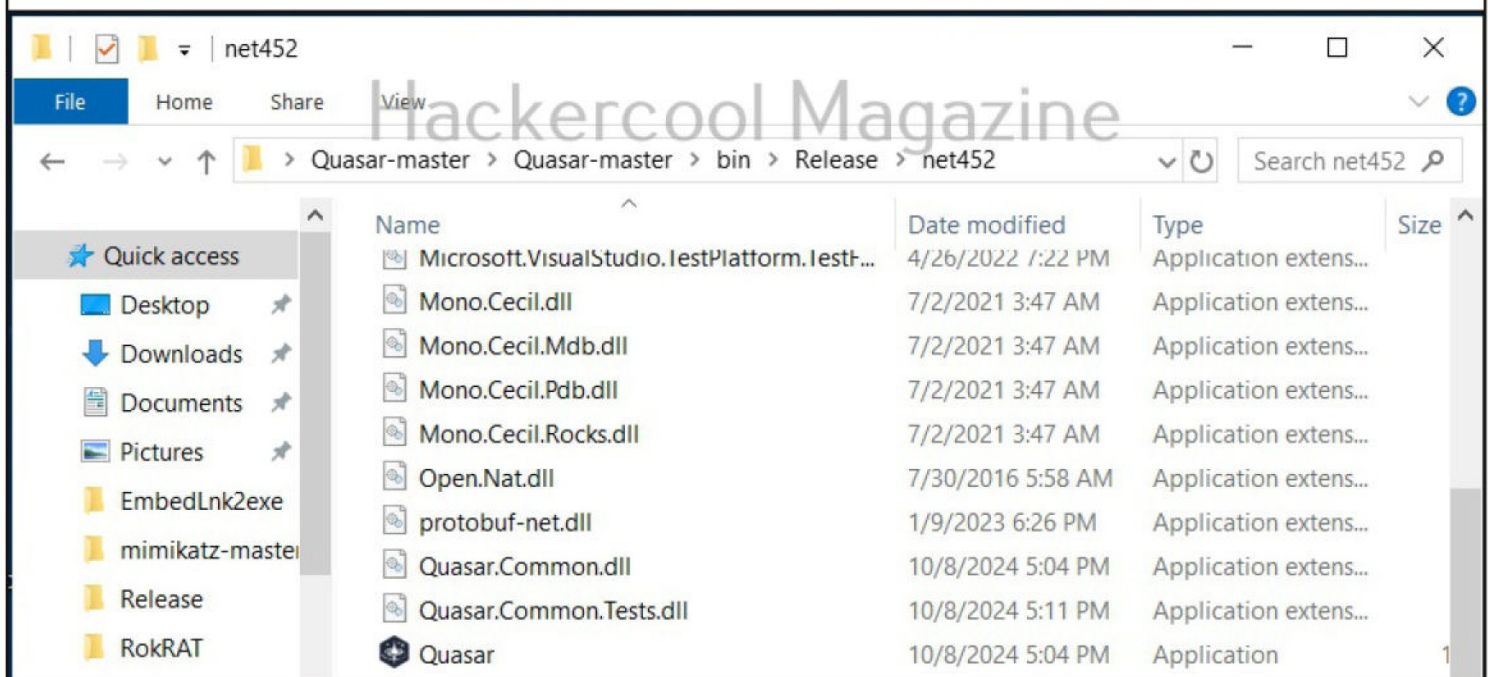
File Name: Name of the project file.

Status Bar: Build succeeded

Once compilation is finished, there will be a new folder named “bin” in the same directory that contains the extracted contents of Quasar RAT. Inside that “bin” folder there will be two folders: tab and release.

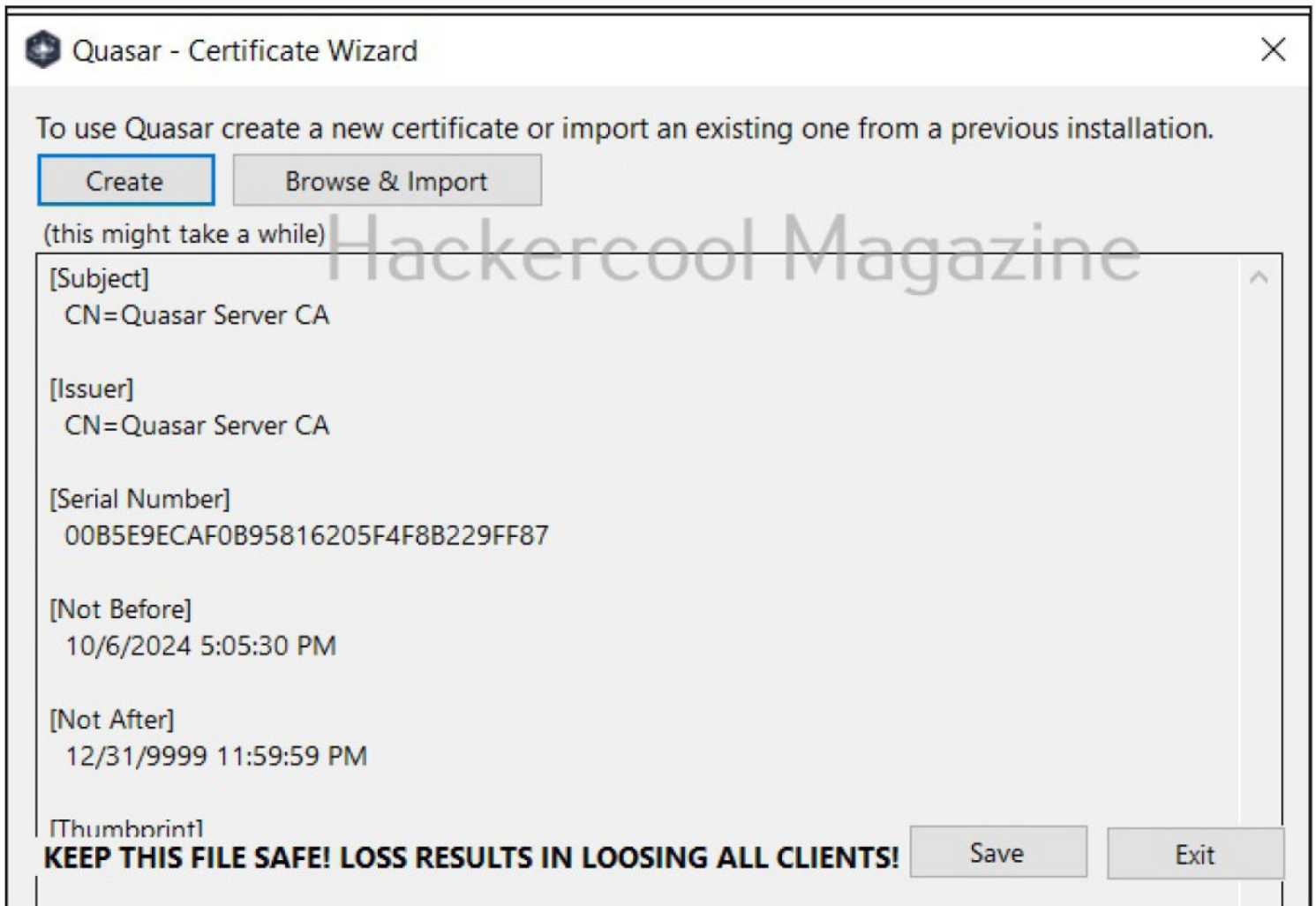


Inside the release folder, you will find the compiled executable of Quasar server. Its named Quasar.

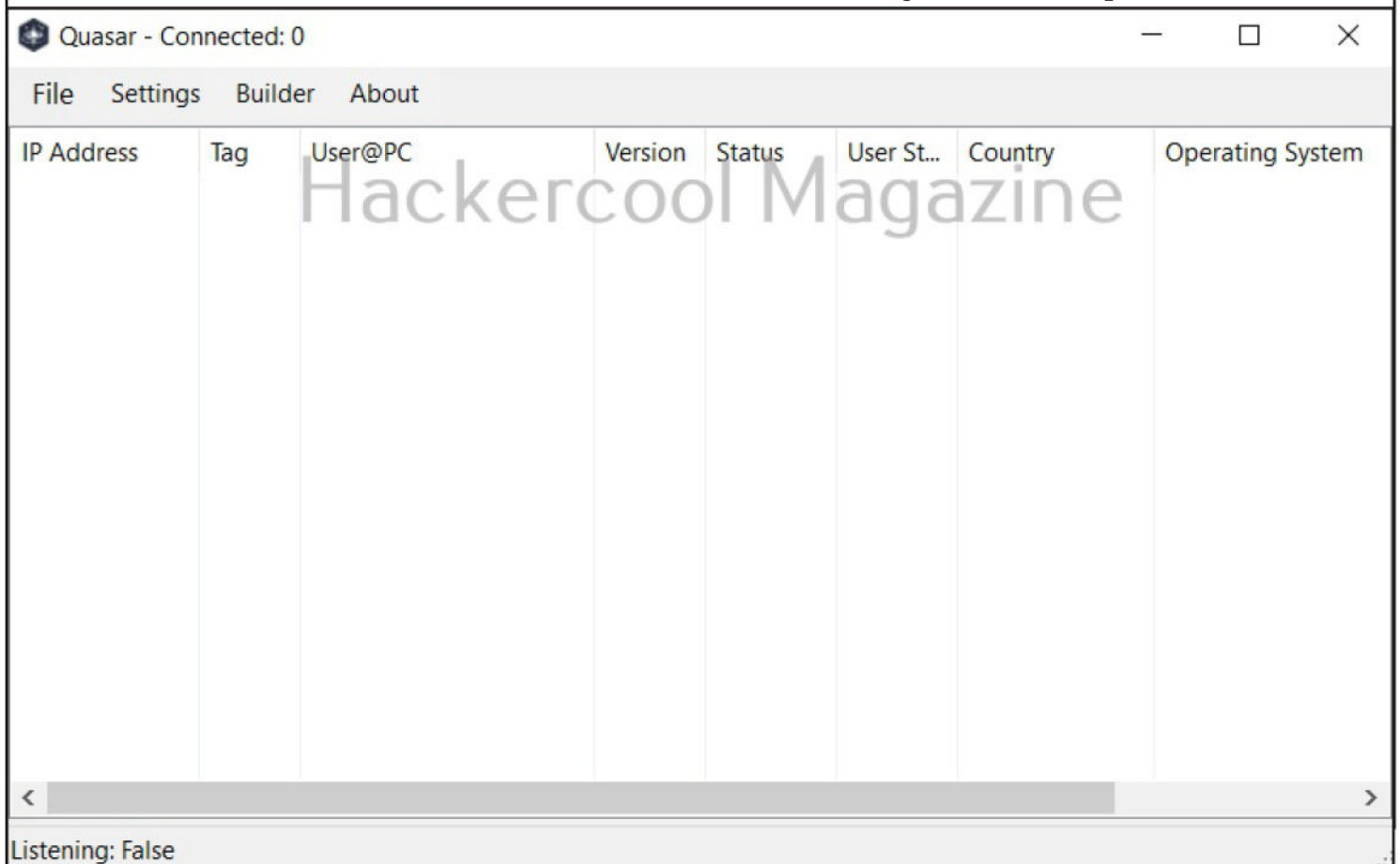


Click on the Quasar application to open the Quasar Server. When you open it for the first time, you will be prompted with a Quasar certificate wizard as shown in the image given below.

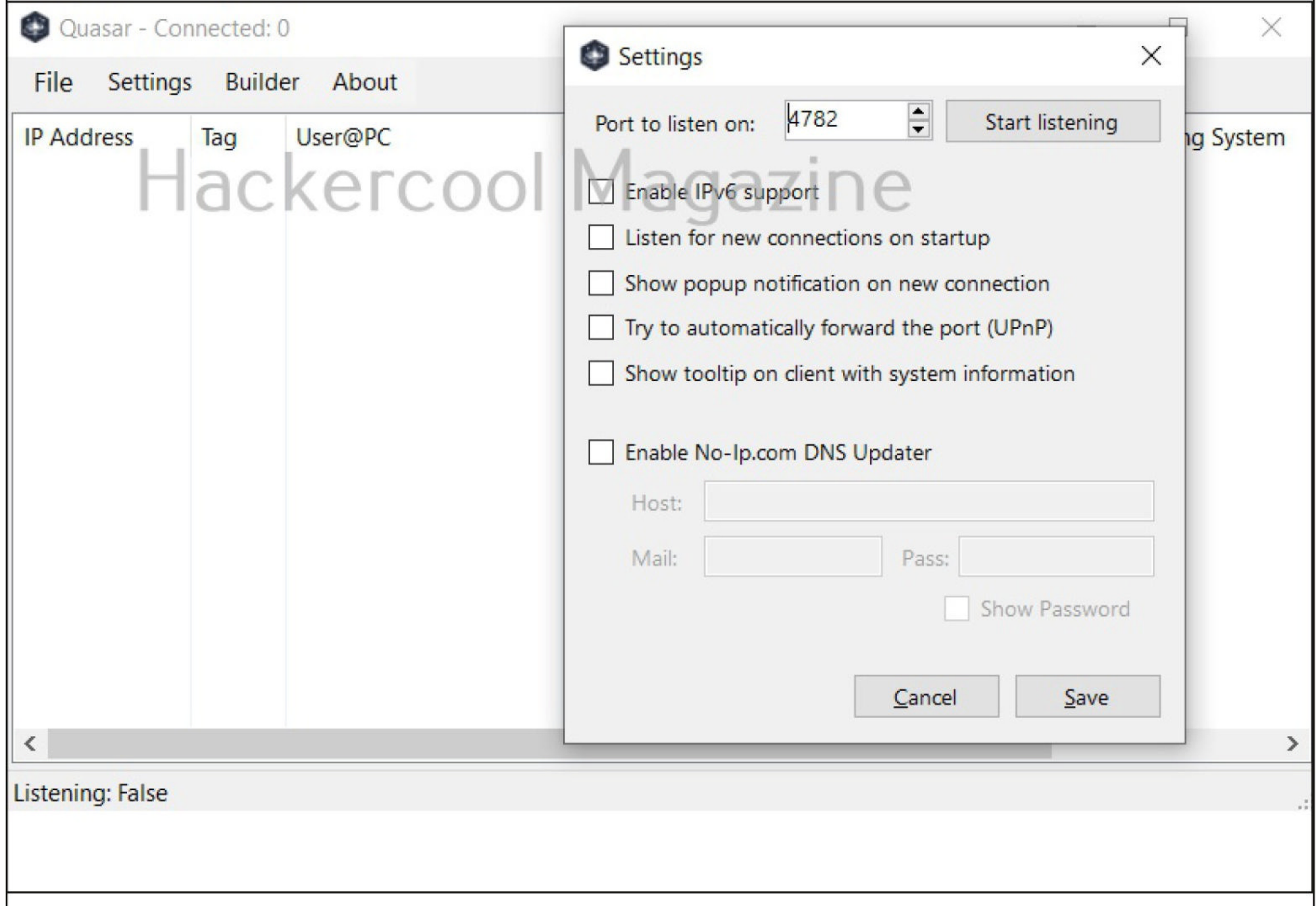




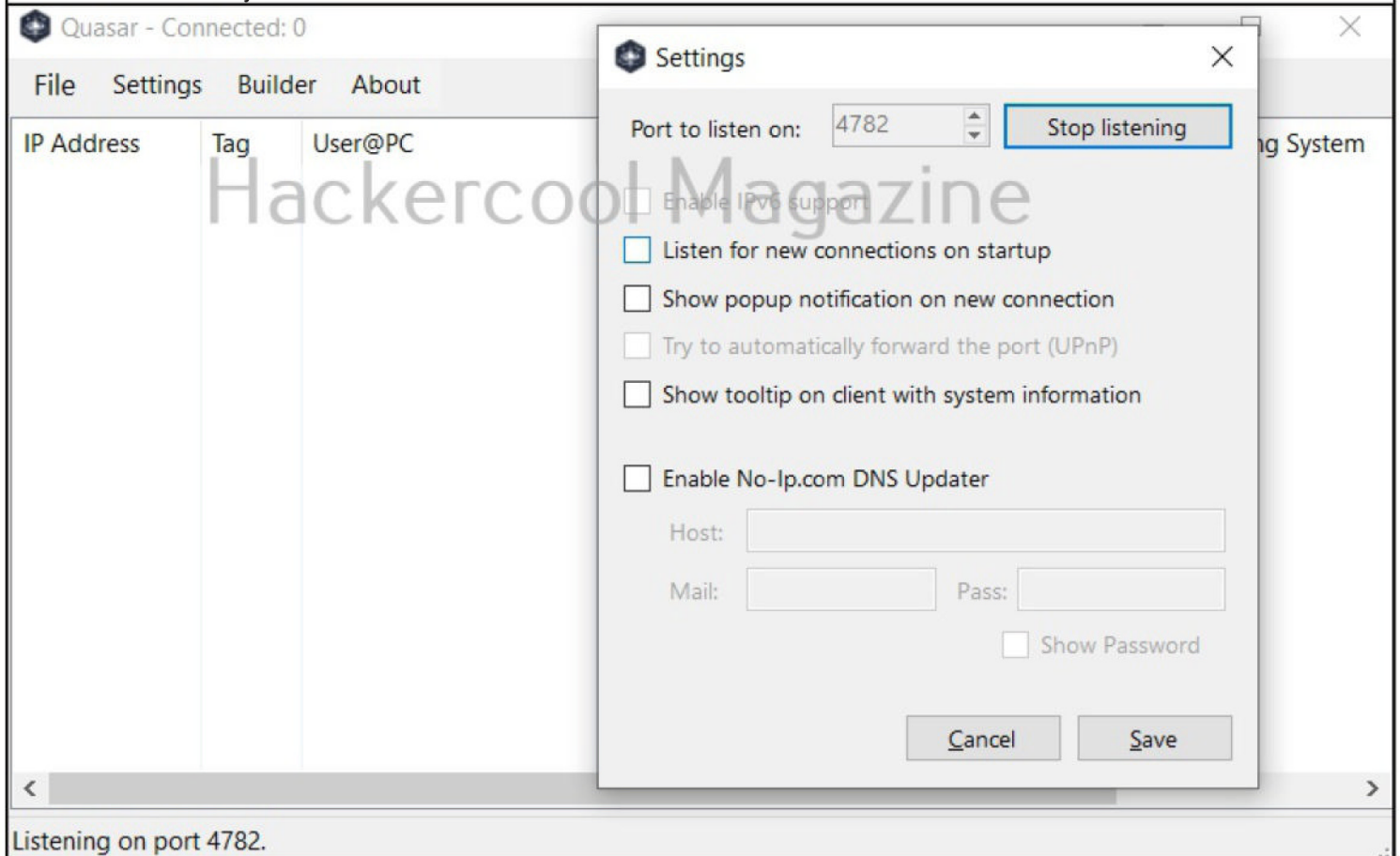
Once the certificate is created, save it to a safe location. The Quasar server opens.



Here, you can see that, it has no clients connected to it. Before creating the Quasar client, let's keep Quasar Server in listening mode. Click on "Settings".



A new window will open. By default, Quasar server listens on port 4782. You can change it depending on your situation and access. Quasar RAT supports features like IPV6, starting on startup, automatic port forwarding etc. After selecting the options, you require, click on “Start listening”. The listener is ready.



Save and close the window. It's time to create the client. Click on “Builder”.



The screenshot shows a window titled "Client Builder" with a close button (X) in the top right corner. On the left is a sidebar with five settings categories: "Basic Settings" (highlighted), "Connection Settings", "Installation Settings", "Assembly Settings", and "Monitoring Settings". The main area displays the "Basic Settings" configuration. It includes a "Client Identification" section with a description and a text input for "Client Tag" containing "Office04". Below this is a "Process Mutex" section with a description and a text input for "Mutex" containing a GUID, with a "Random Mutex" button to its right. At the bottom of the main area is an "Unattended mode" section with a checkbox labeled "Enable unattended mode". A "Build Client" button is located at the bottom right of the window.

Client Builder

Basic Settings

Client Identification
You can choose a tag to identify your client.

Client Tag:

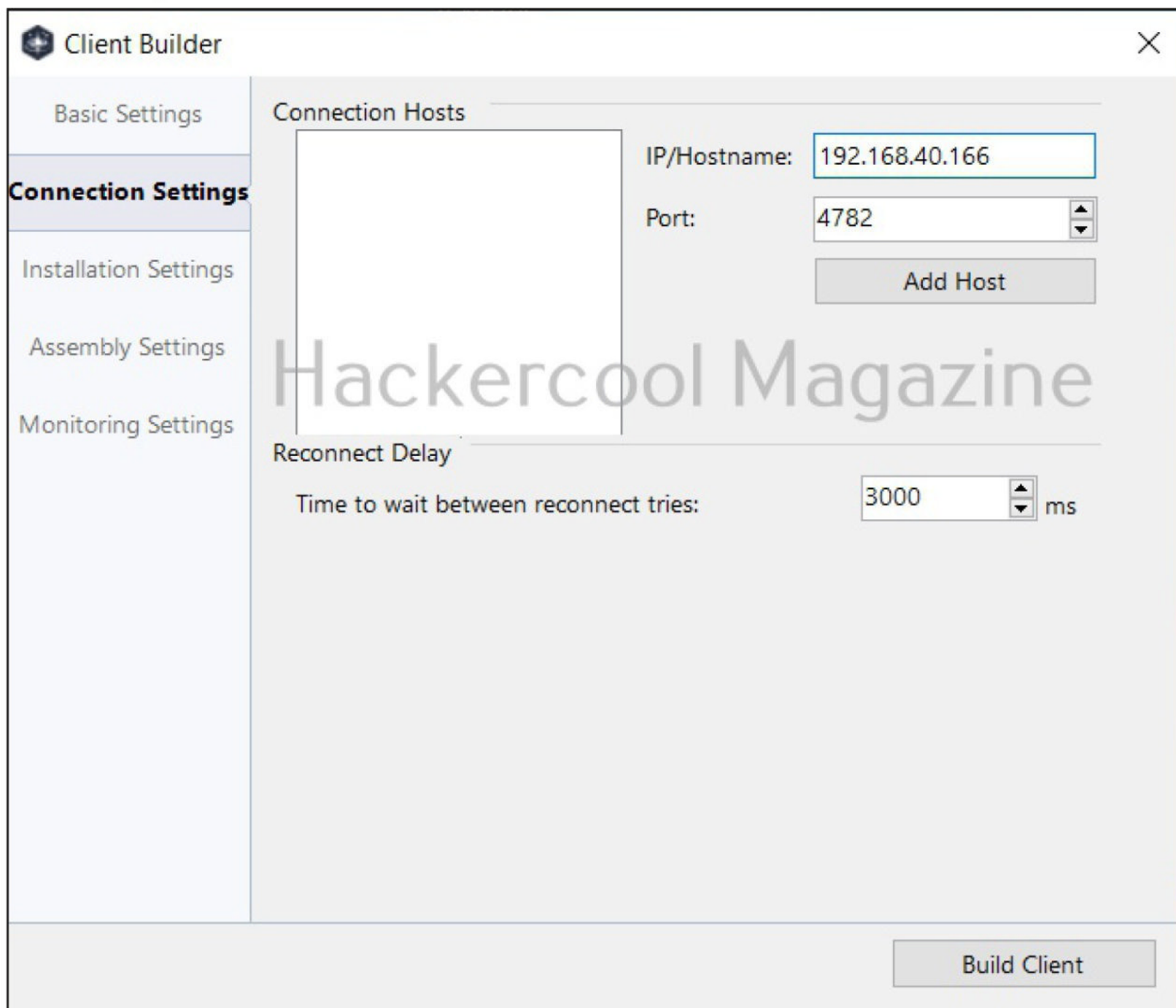
Process Mutex
A unique mutex ensures that only one instance of the client is running on the same system.

Mutex:

Unattended mode
Activating the unattended mode allows remote control of the client without user interaction.

☐ Enable unattended mode

Giving tags to the client can make it easy for identifying clients. Go to “Connection Settings”. Give the IP of the machine on which the Quasar Server is running and click on “Add Host”.



The screenshot shows the 'Client Builder' application window. On the left is a sidebar with navigation tabs: 'Basic Settings', 'Connection Settings' (which is selected and highlighted in blue), 'Installation Settings', 'Assembly Settings', and 'Monitoring Settings'. The main area of the window is titled 'Connection Hosts'. It contains a large empty rectangular box for a list of hosts. To the right of this box are two input fields: 'IP/Hostname:' with the value '192.168.40.166' and 'Port:' with the value '4782'. Below these fields is an 'Add Host' button. At the bottom of the main area, there is a 'Reconnect Delay' section with the label 'Time to wait between reconnect tries:' and a spinner box containing the value '3000' followed by 'ms'. A large, semi-transparent watermark 'Hackercool Magazine' is overlaid across the center of the window. At the bottom right corner, there is a 'Build Client' button.

Client Builder

Basic Settings

Connection Settings

Installation Settings

Assembly Settings

Monitoring Settings

Connection Hosts

IP/Hostname: 192.168.40.166

Port: 4782

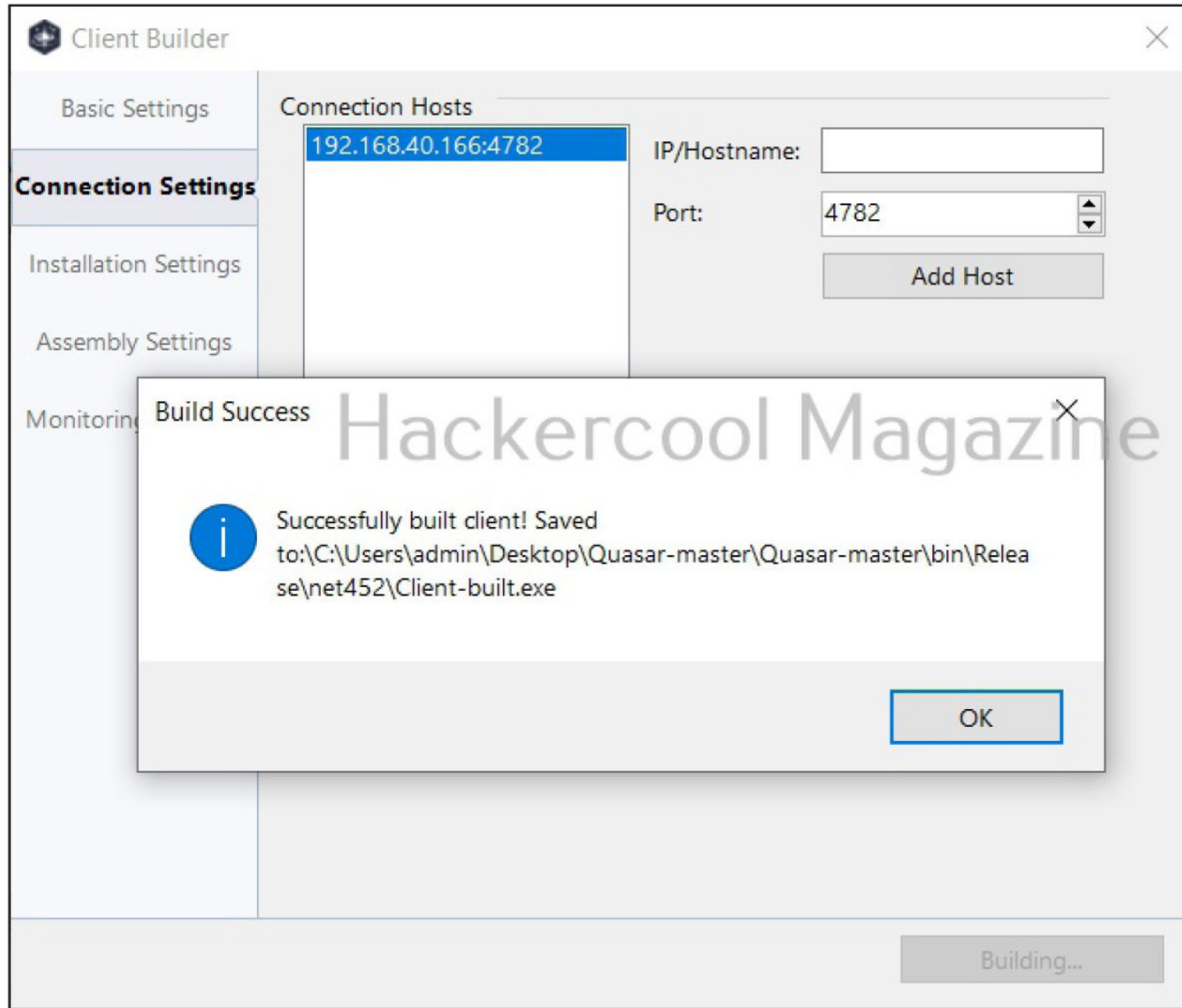
Add Host

Reconnect Delay

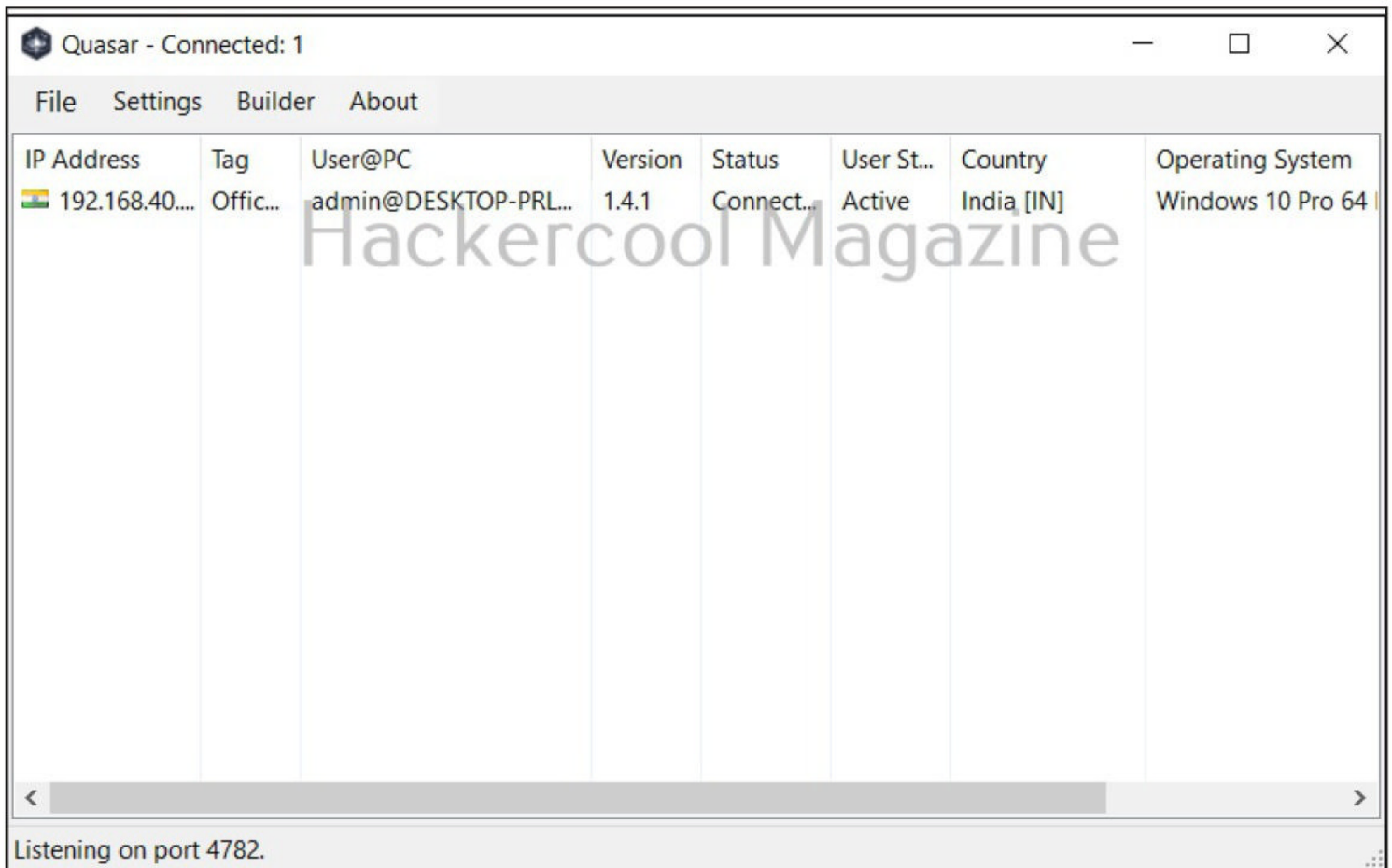
Time to wait between reconnect tries: 3000 ms

Build Client

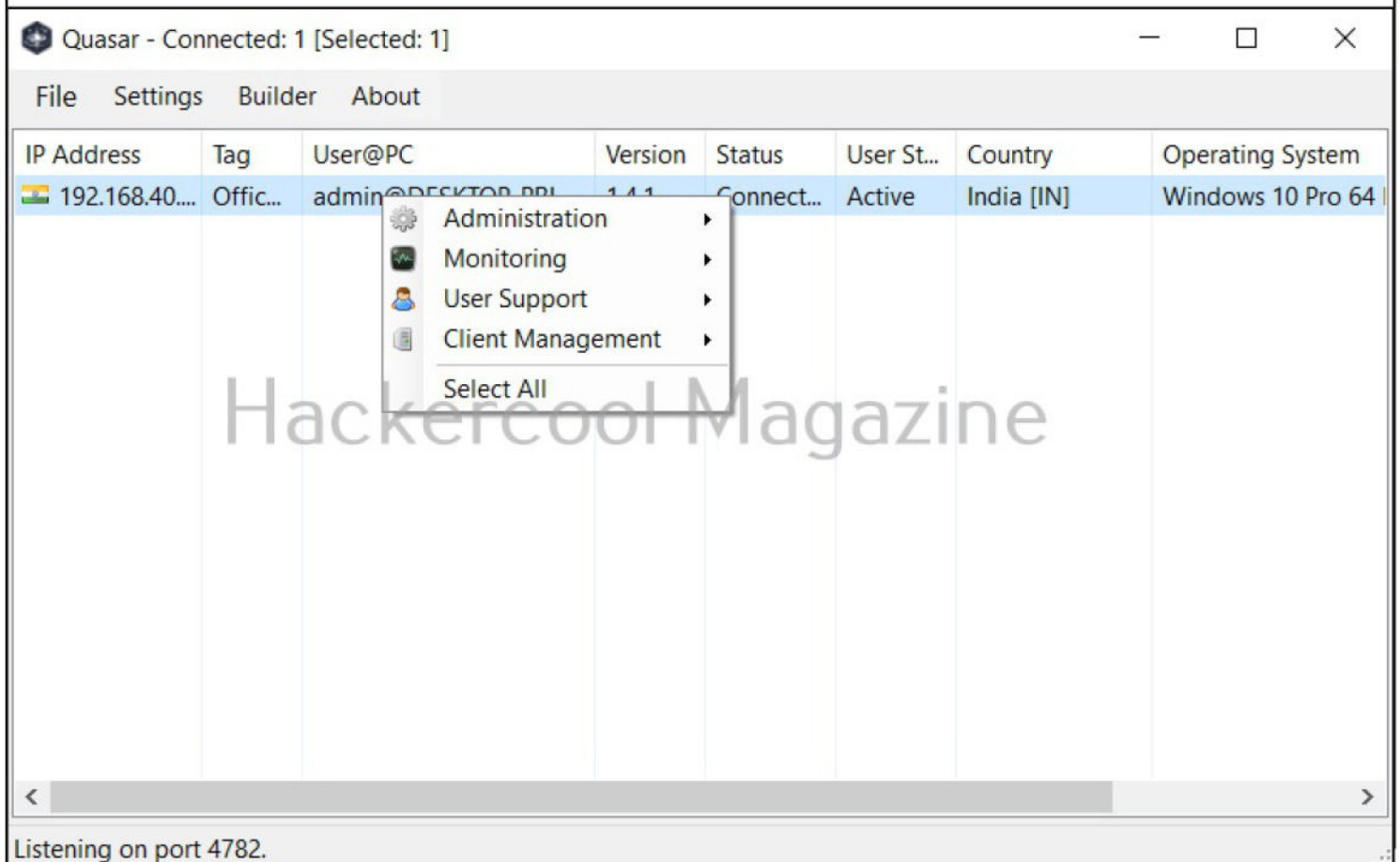
Then click on “save”.



The client executable will be located in the same folder as the Quasar Server was. Now, this file needs to be sent to the target user. When the target user clicks on this “client.exe” file, we get a connection from the client as shown below.



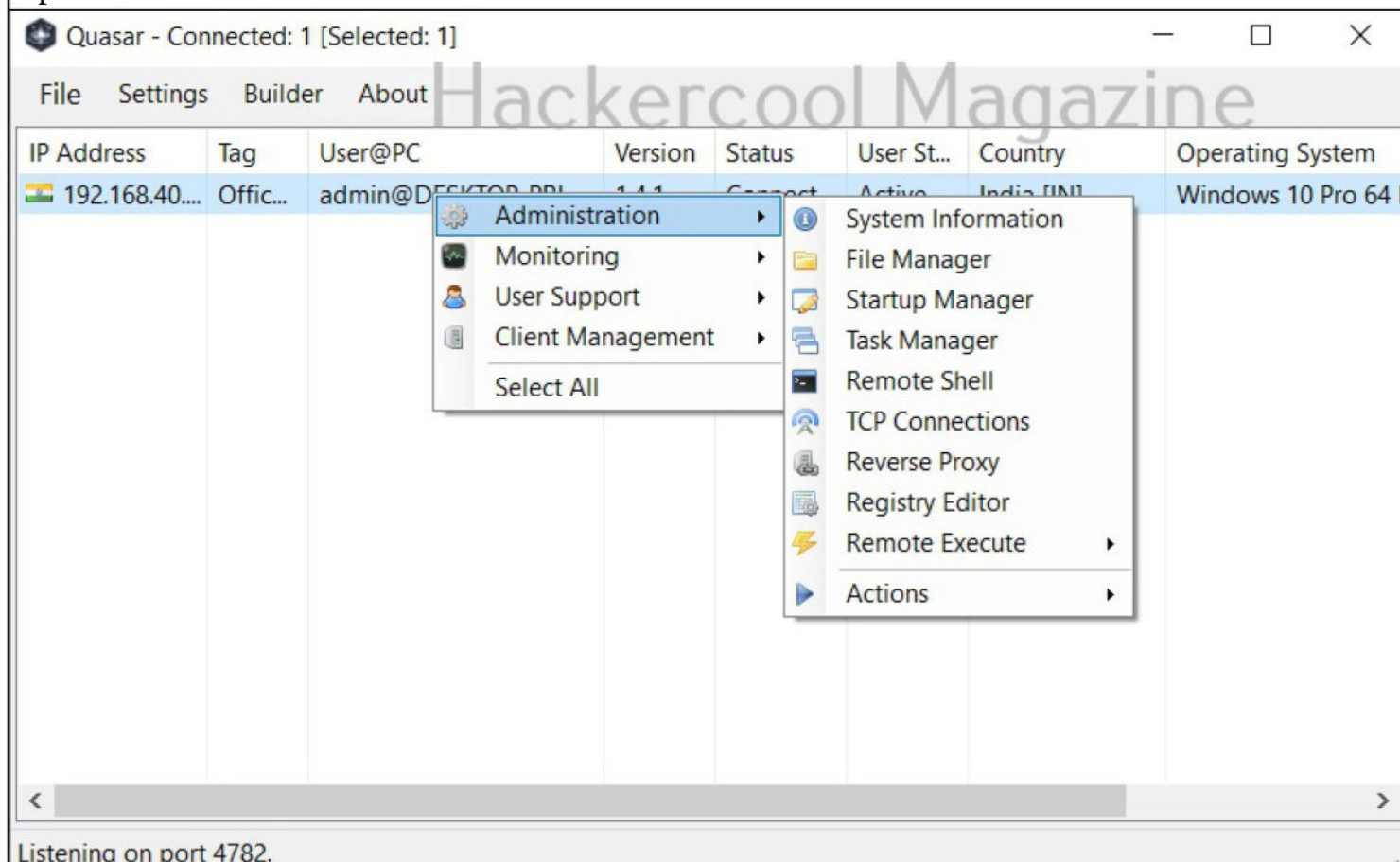
Since we now have the connection from a client, let's see what all we can do with Quasar RAT on the target system. Right click on the connection as shown below and this will reveal a menu as shown below.



The items of this menu are,

- 1) Administration
- 2) Monitoring
- 3) User support and
- 4) Client management

Hovering on a specific menu with mouse reveals its submenu which has a list of functions you can perform.



Listening on port 4782.

Let's learn about each of these functions, one by one. The first function is "system information" function and as its name implies, selecting this function reveals all the information about the target system.

DID YOU KNOW?

Users from many countries of the world can subscribe to Hackercool Magazine using their local currency now.

System Information - admin@DESKTOP-PRLKILM [192.168.40.150:50049]

Component	Value
Operating System	Windows 10 Pro 64 Bit
Architecture	x64 (64 Bit)
Processor (CPU)	Intel(R) Core(TM) i3-10110U CPU @ 2.10GHz; Intel(R) Core(TM) i3-10110U CPU @ 2
Memory (RAM)	2047 MB
Video Card (GPU)	VMware SVGA 3D
Username	admin
PC Name	DESKTOP-PRLKILM
Domain Name	-
Host Name	DESKTOP-PRLKILM
System Drive	C:\
System Directory	C:\Windows\system32
Uptime	0d : 0h : 14m : 30s
MAC Address	00:0C:29:35:A4:D1
LAN IP Address	192.168.40.150
WAN IP Address	49.205.114.232

With the “File Management” function, you can manage the files on the target system.

File Manager - admin@DESKTOP-PRLKILM [192.168.40.150:50049]

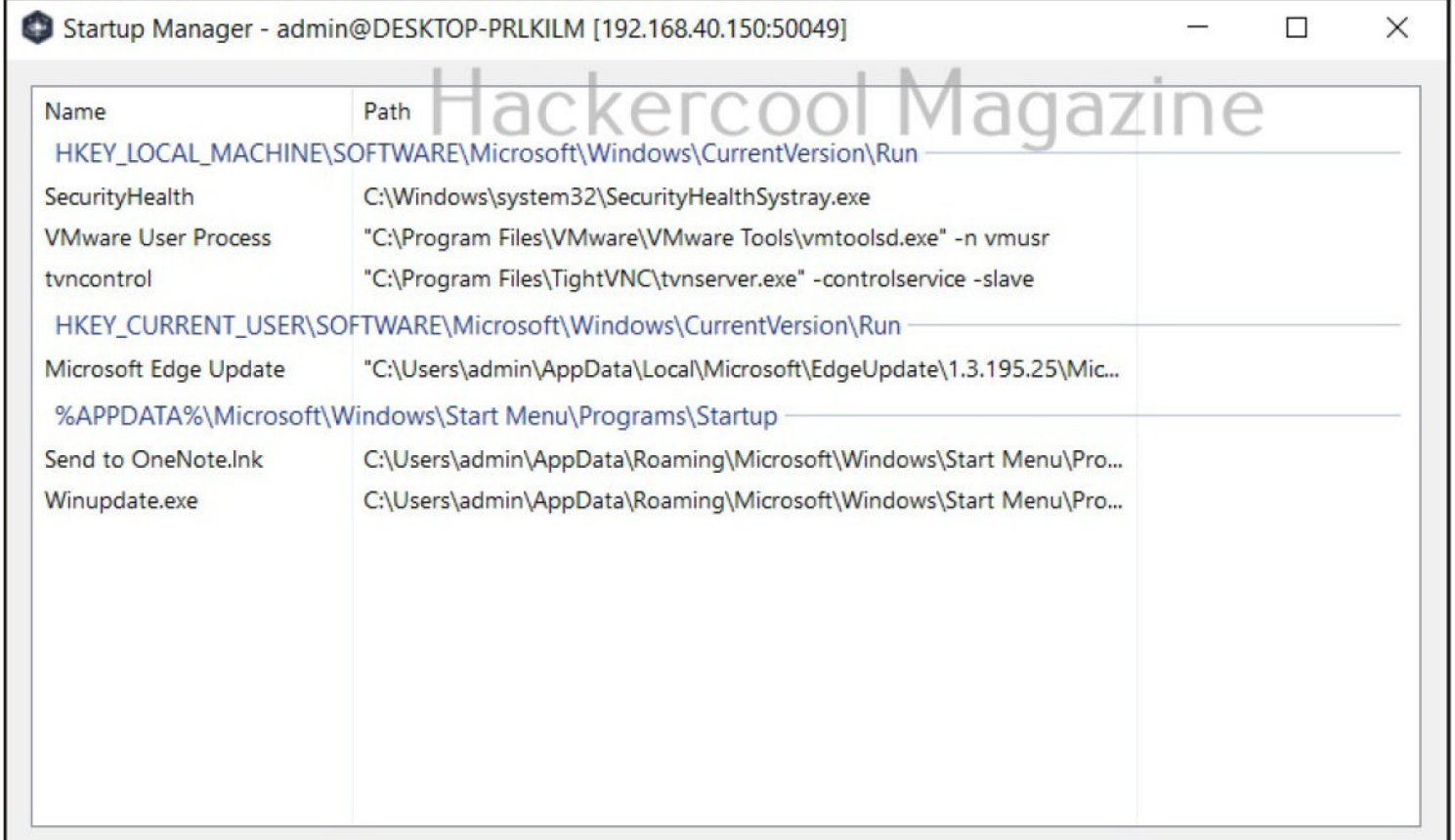
File Explorer

Drive: C:\ [Local Disk, NTFS] Remote Path: C:\

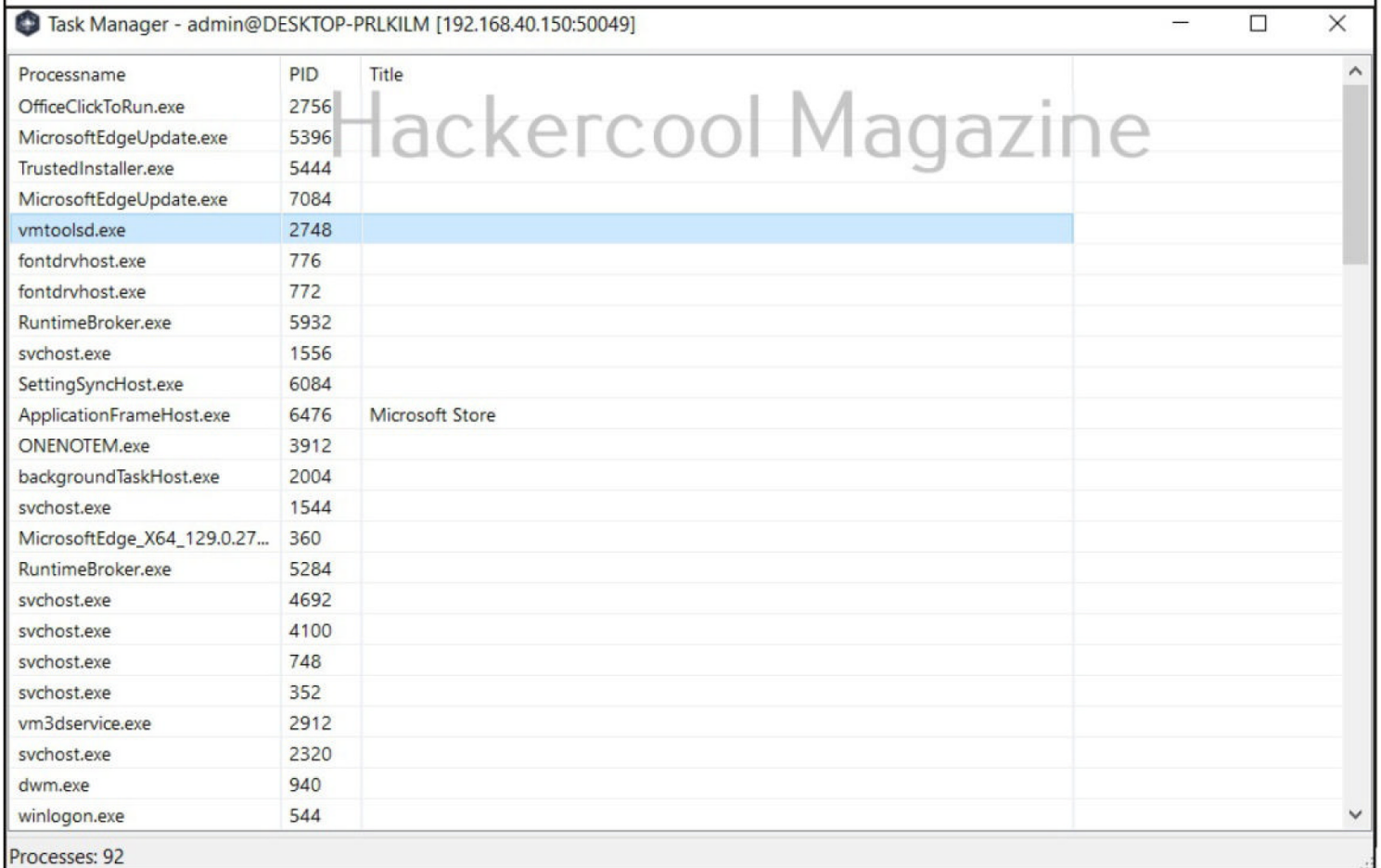
Name	Size	Type
..		
\$Recycle.Bin		Directory
CouchDB		Directory
Documents and Settings		Directory
OneDriveTemp		Directory
PerfLogs		Directory
Program Files		Directory
Program Files (x86)		Directory
ProgramData		Directory
Recovery		Directory
System Volume Information		Directory
Users		Directory
Windows		Directory
Hc_Decoy.pdf	13.71 KB	File
hc_test2.bat	128 B	File
pagefile.sys	1.3 GB	File
swapfile.sys	16 MB	File

Status: Ready

The “Startup manager” will show you all the programs on the target system that start as soon as the target system starts.



Similarly, with “Task Manager” you can see all the processes running on the target system along with their PID.



With “Remote Shell” feature, you can open a remote shell to the target system.



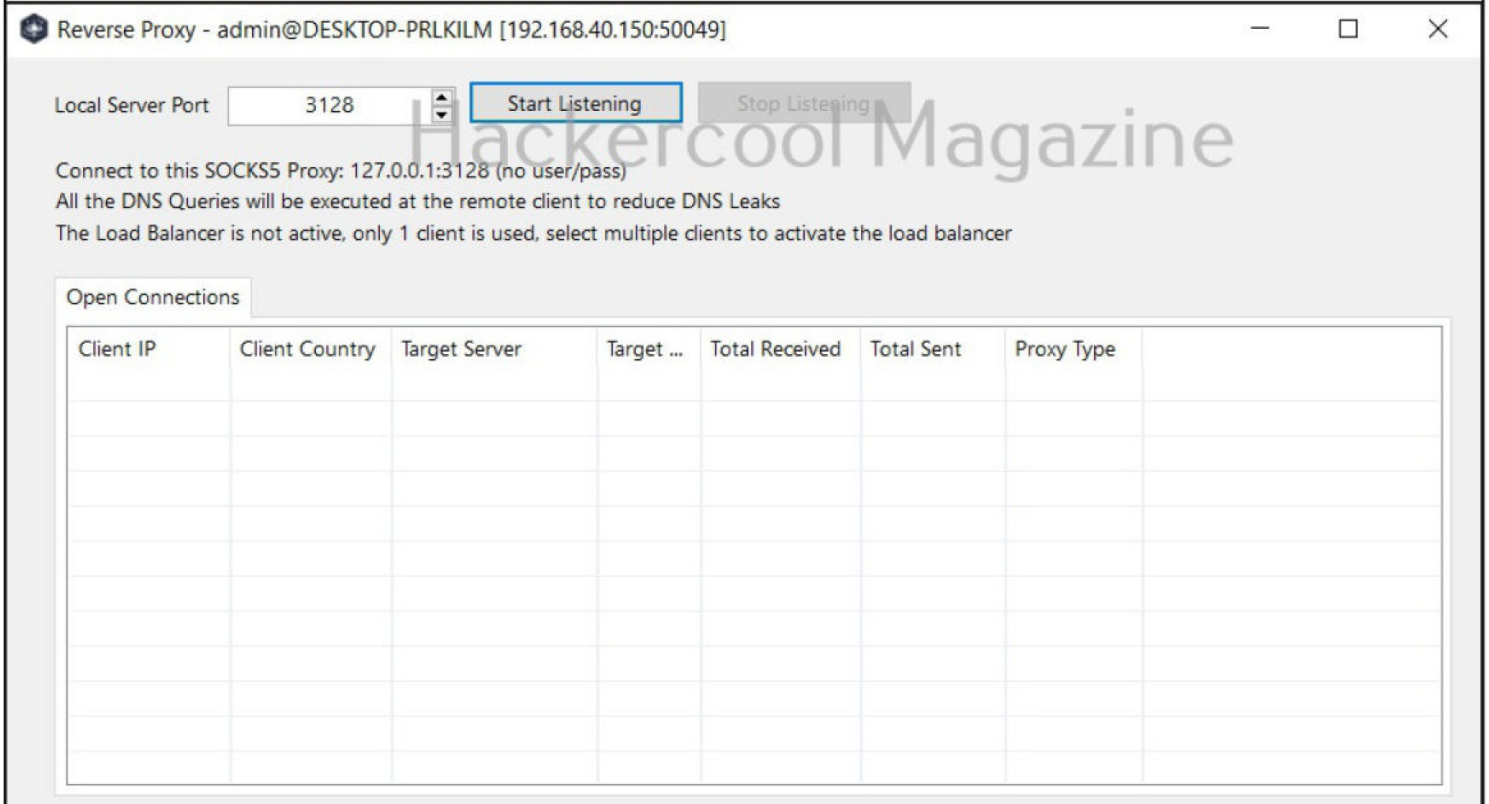
The “TCP connections” feature shows all the connections to and from the target system.

Connections - admin@DESKTOP-PRLKILM [192.168.40.150:50049]

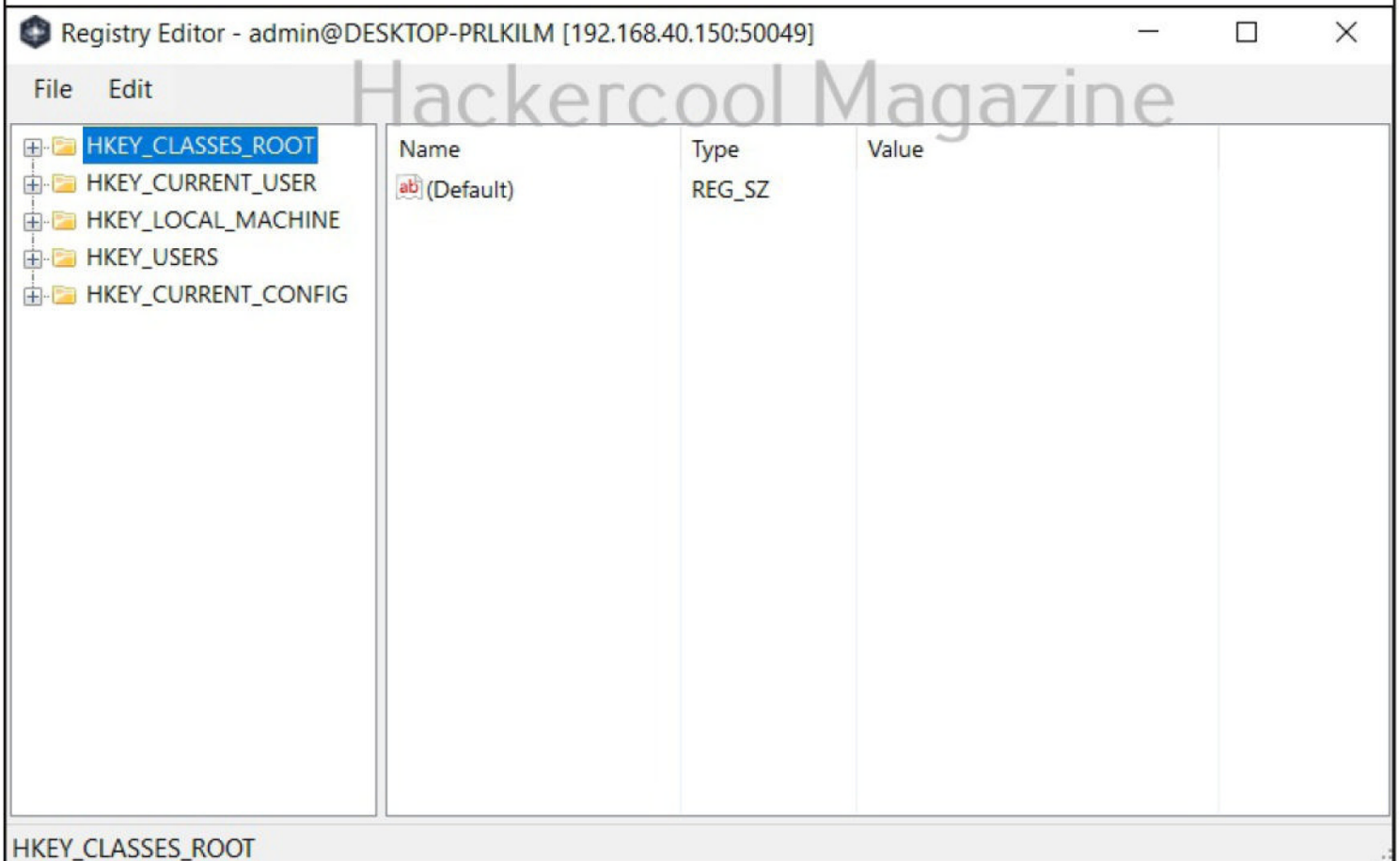
Process	Local Address	Local Port	Remote Address	Remote Port	State
Listening					
svchost	0.0.0.0	135	0.0.0.0	0	Listening
System	0.0.0.0	445	0.0.0.0	0	Listening
svchost	0.0.0.0	5040	0.0.0.0	0	Listening
tvnserver	0.0.0.0	5800	0.0.0.0	0	Listening
tvnserver	0.0.0.0	5900	0.0.0.0	0	Listening
svchost	0.0.0.0	7680	0.0.0.0	0	Listening
pc-print-deploy-server	0.0.0.0	9173	0.0.0.0	0	Listening
pc-print-deploy-server	0.0.0.0	9174	0.0.0.0	0	Listening
pc-app	0.0.0.0	9191	0.0.0.0	0	Listening
pc-app	0.0.0.0	9192	0.0.0.0	0	Listening
pc-app	0.0.0.0	9193	0.0.0.0	0	Listening
pc-app	0.0.0.0	9195	0.0.0.0	0	Listening
wininit	0.0.0.0	49664	0.0.0.0	0	Listening
svchost	0.0.0.0	49665	0.0.0.0	0	Listening
lsass	0.0.0.0	49666	0.0.0.0	0	Listening
svchost	0.0.0.0	49667	0.0.0.0	0	Listening
spoolsv	0.0.0.0	49668	0.0.0.0	0	Listening
svchost	0.0.0.0	49669	0.0.0.0	0	Listening
services	0.0.0.0	49698	0.0.0.0	0	Listening

You can even start a reverse proxy on the target system using Quasar with the function with the

same name. Quasar creates a SOCKS5 proxy.



With the “Registry Editor”, you can make changes to the Windows Registry of the target system.



You can even execute files on the target system using Quasar RAT using the “Remote execution”

feature. The file you want to execute on the target system can be on your attacker system or on an external URL.

Remote Execution [Selected: 1]

Execute local file

Path:

Browse...

Execute from URL

URL:

Client	Status	
admin@DESKTOP-PRLKILM [192.168.40.150:...	Waiting...	

Update clients with this file

Execute remotely

QuasarRAT is also known by names CinaRAT and Yggdrasil.

Remote Execution [Selected: 1]

☐ Execute local file

Path:

Browse...

☒ Execute from URL

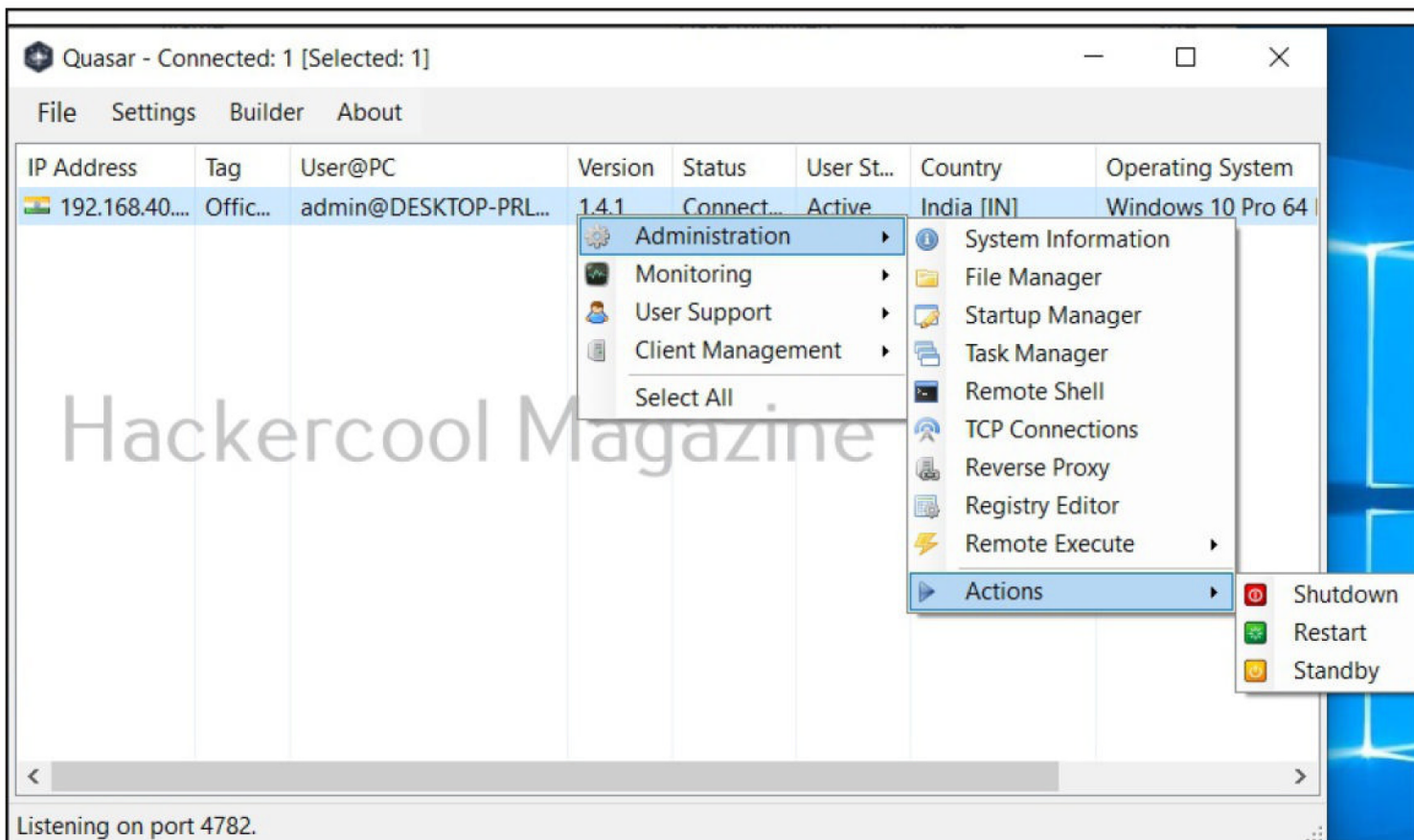
URL:

Client	Status
admin@DESKTOP-PRLKILM [192.168.40.150:...]	Waiting...

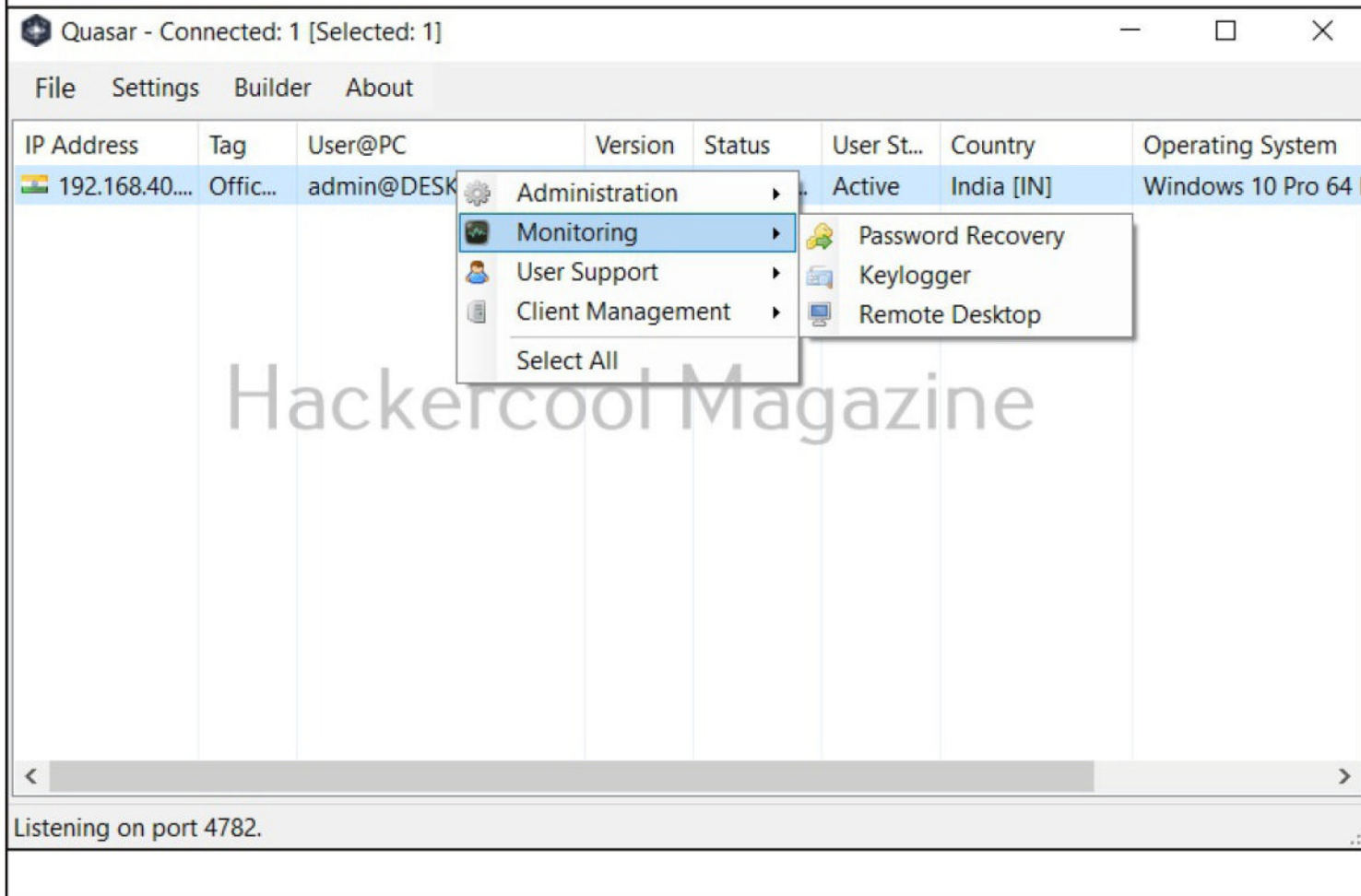
☐ Update clients with this file Execute remotely

You can even shutdown, restart and keep the system in standby mode with Quasar RAT.

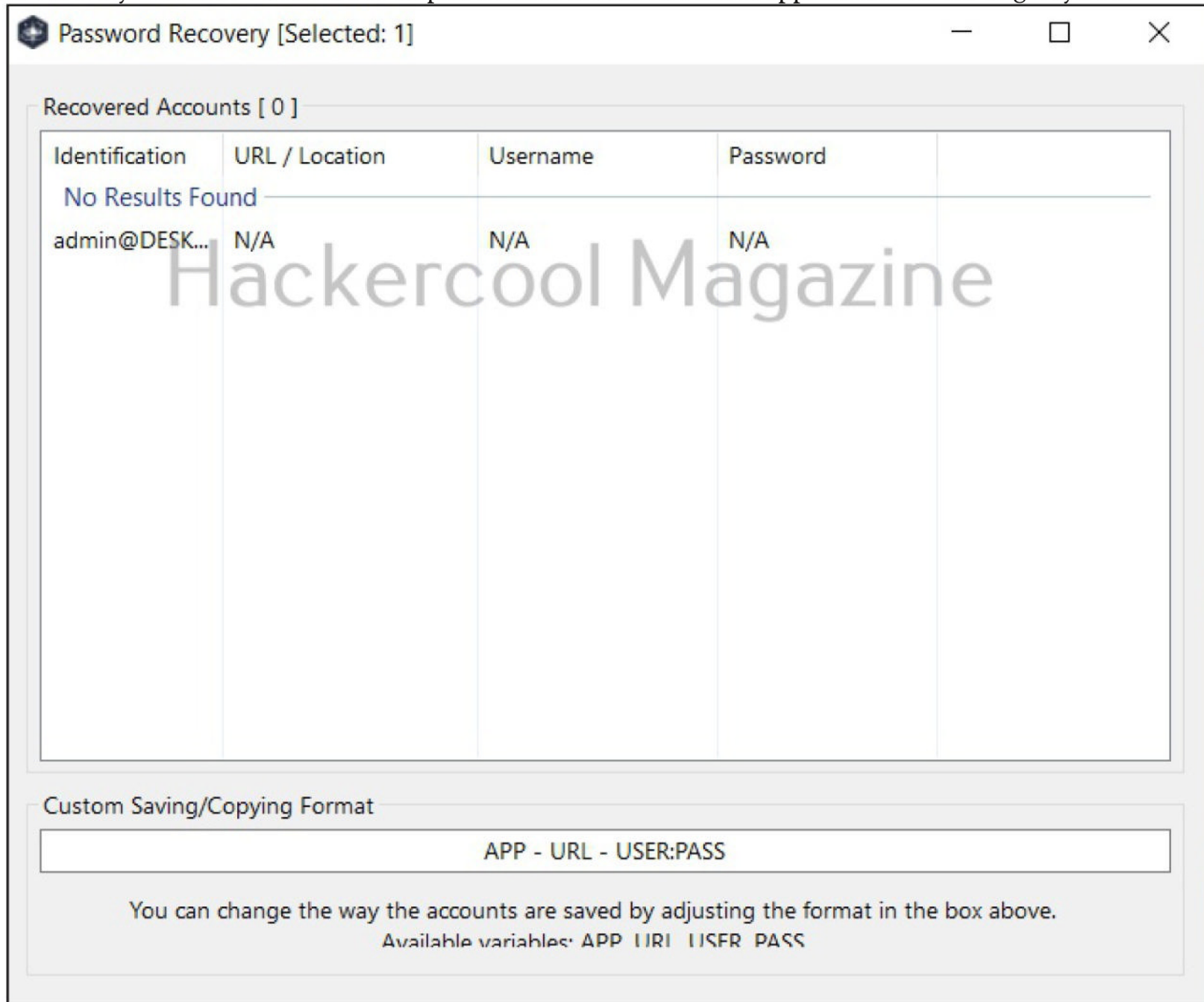
A threat actor being tracked as Blind Eagle used a customized version of Quasar RAT to target Colombian insurance sector as recently as September 2024.



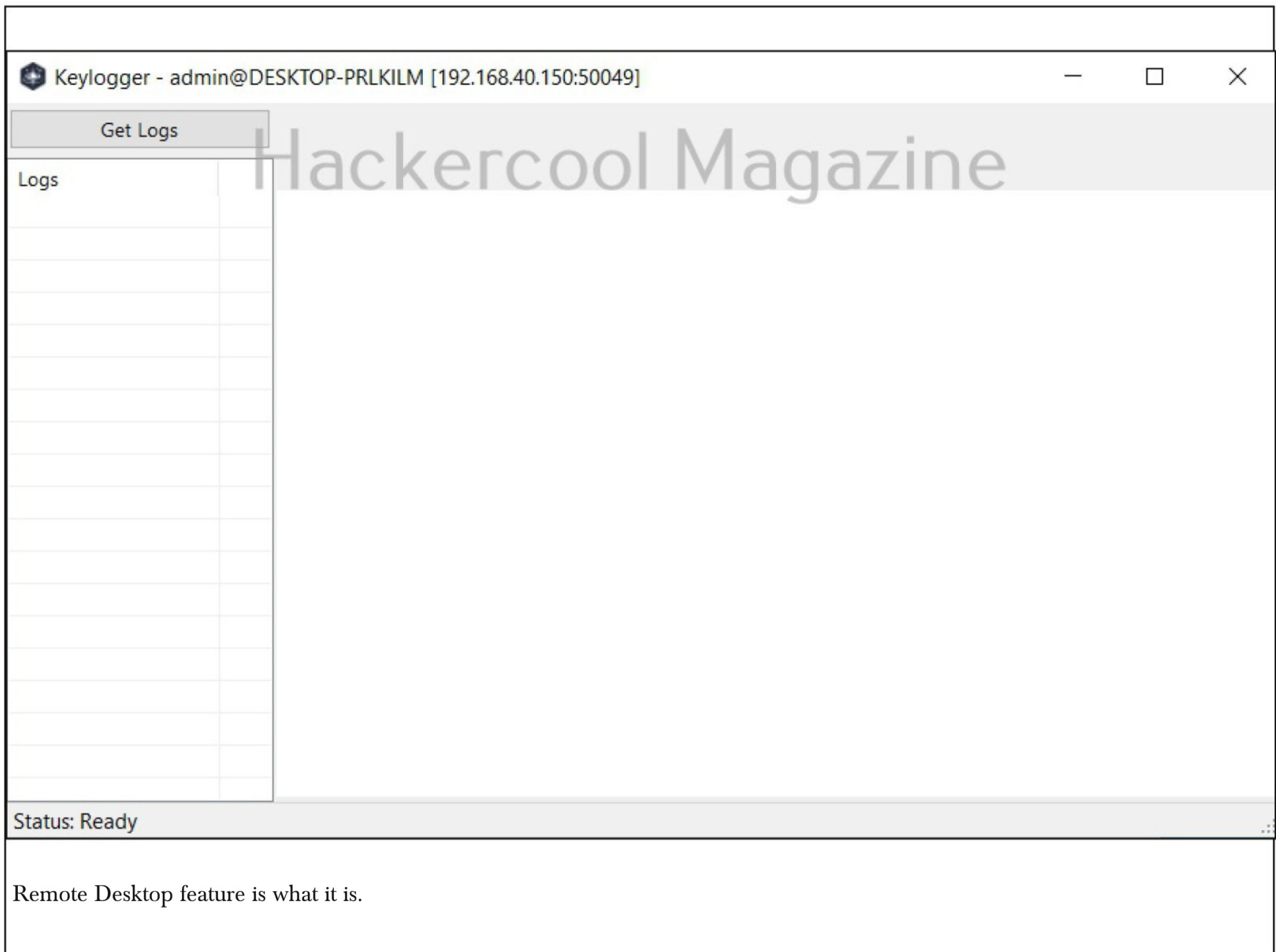
The “Monitoring” menu of Quasar RAT has all the functions that can be used to monitor the target systems. Let’s see each function.

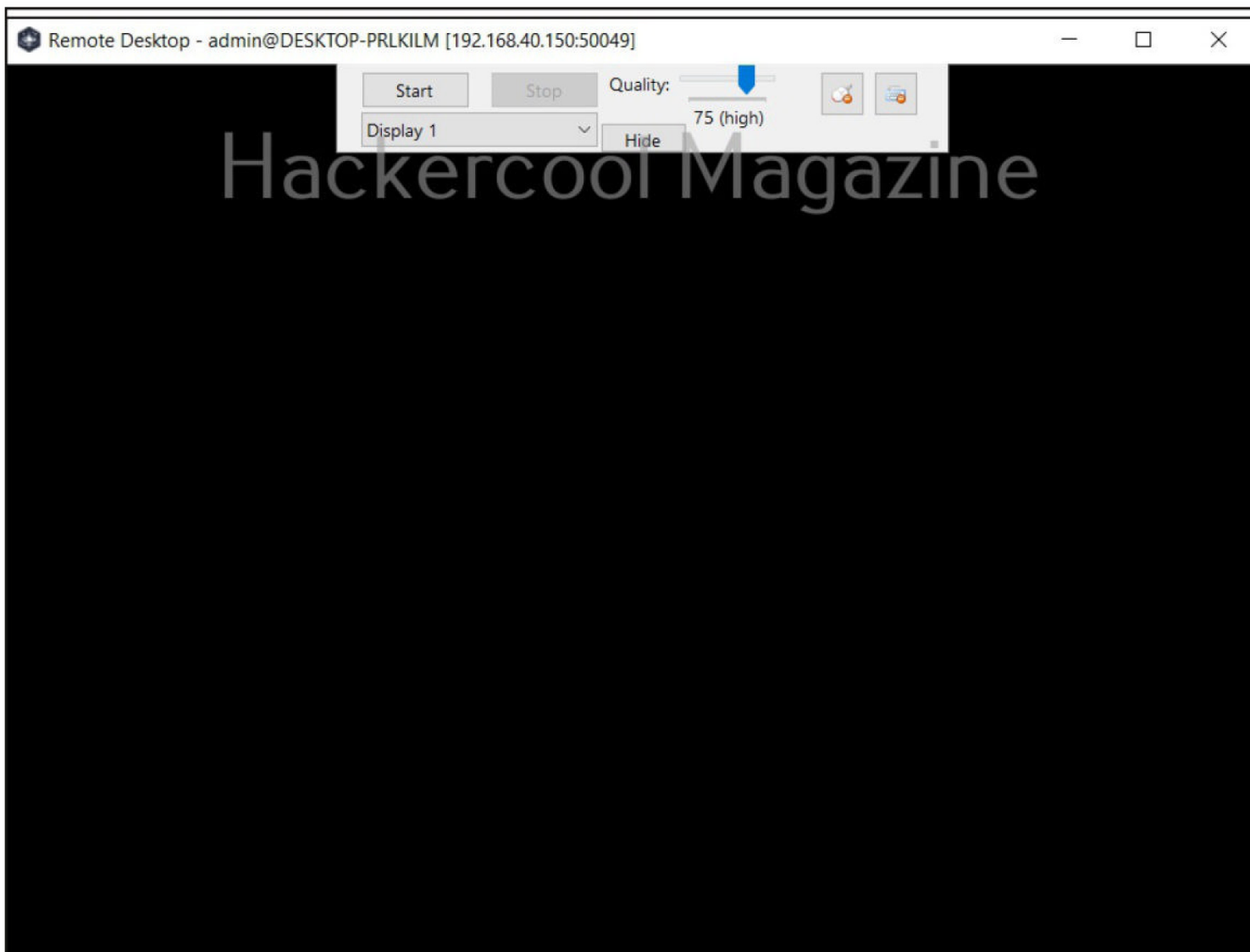


The “Password recovery” function retrieves stored passwords from browsers and applications on the target system.

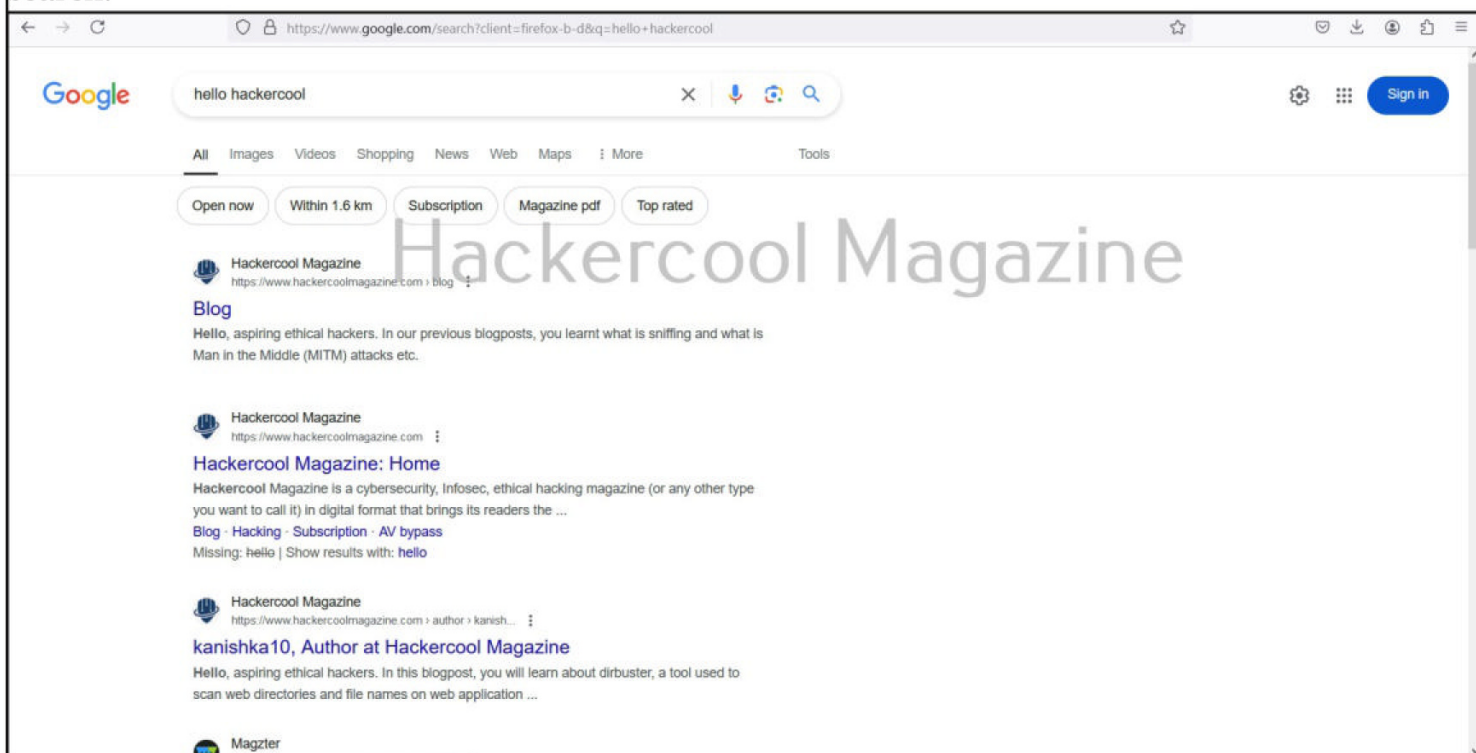


The keylogger function logs keystrokes on the target system.





For example, on the target systems, the user has opened the browser and is doing a Google search.



We can view it remotely using remote desktop.

Remote Desktop - admin@DESKTOP-PRLKILM [192.168.40.150:50049] - FPS: 4.77

aboutsessionrestore x hello hackercool - C Start Stop Quality: 75 (high) Display 1 Hide

Google hello hackercool X Sign in

All Images Videos Shopping News Web Maps More Tools

Open now Within 1.6 km Subscription Magazine pdf Top rated

Hackercool Magazine
<https://www.hackercoolmagazine.com> > Blog

Blog
 Hello, aspiring ethical hackers. In our previous blogposts, you learnt what is sniffing and what is Man in the Middle (MITM) attacks etc.

Hackercool Magazine
<https://www.hackercoolmagazine.com>

Hackercool Magazine: Home
 Hackercool Magazine is a cybersecurity, Infosec, ethical hacking magazine (or any other type you want to call it) in digital format that brings its readers the ...
[Blog](#) · [Hacking](#) · [Subscription](#) · [AV bypass](#)
 Missing: hello | Show results with: hello

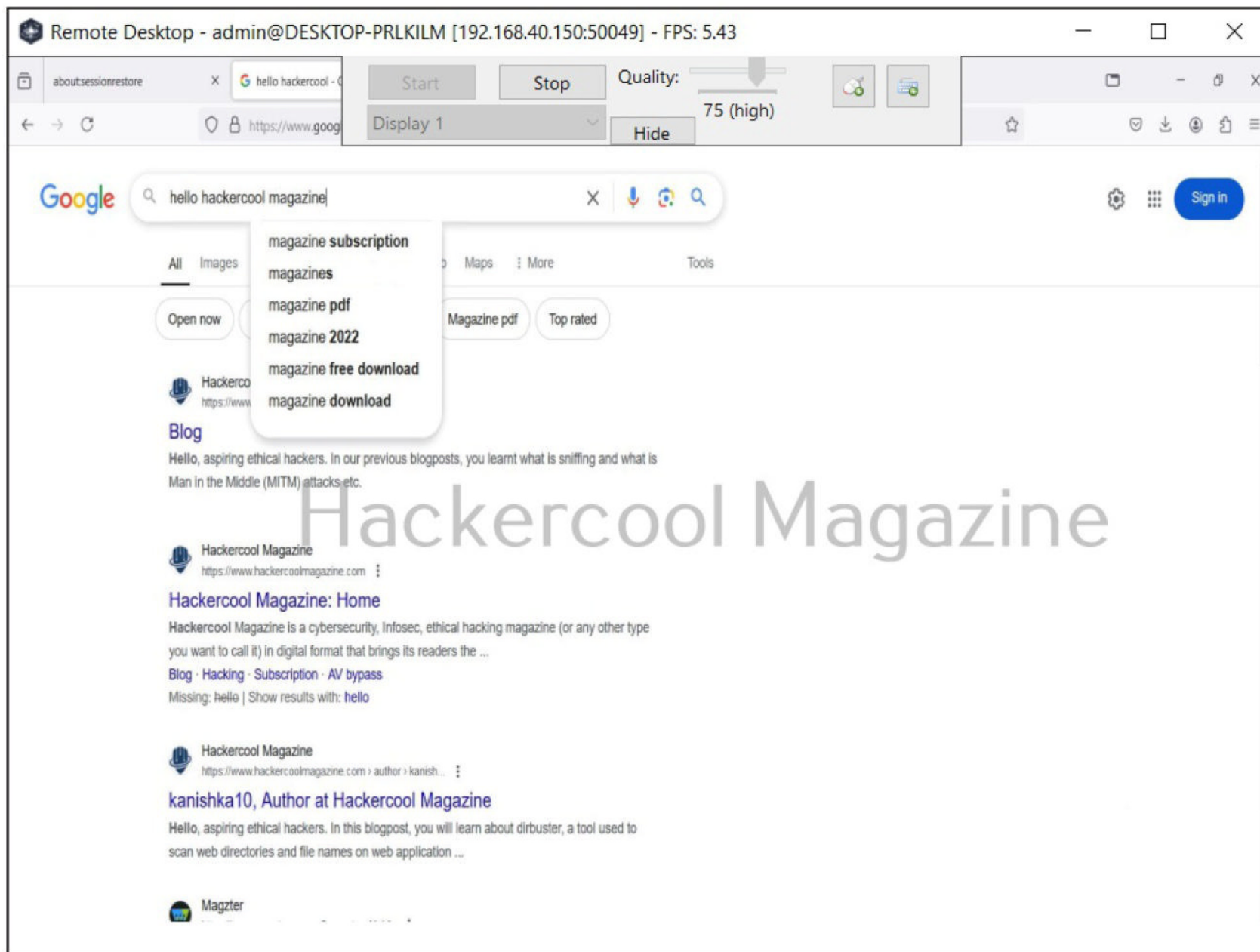
Hackercool Magazine
<https://www.hackercoolmagazine.com> > author > kanish...

kanishka10, Author at Hackercool Magazine
 Hello, aspiring ethical hackers. In this blogpost, you will learn about dirbuster, a tool used to scan web directories and file names on web application ...

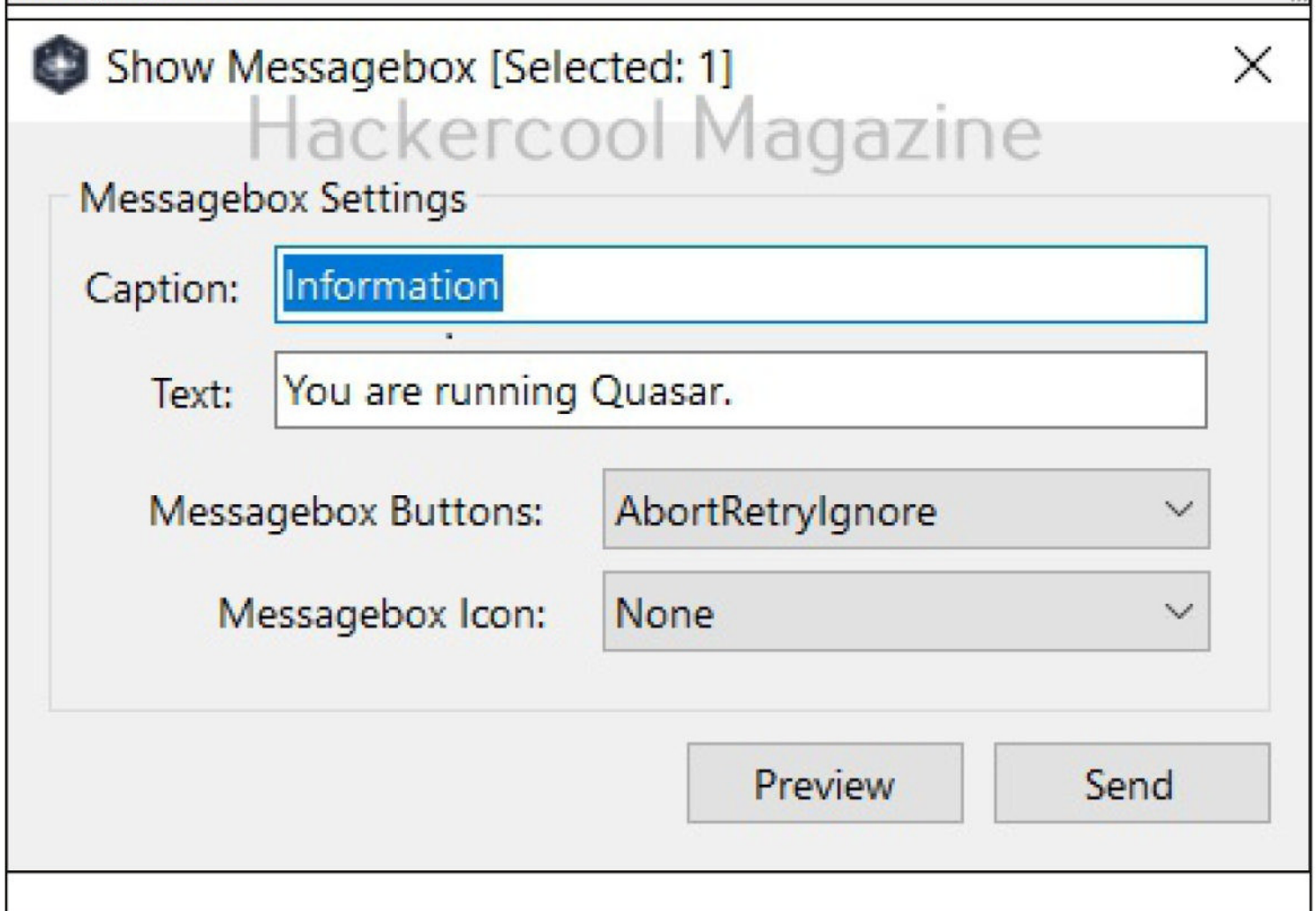
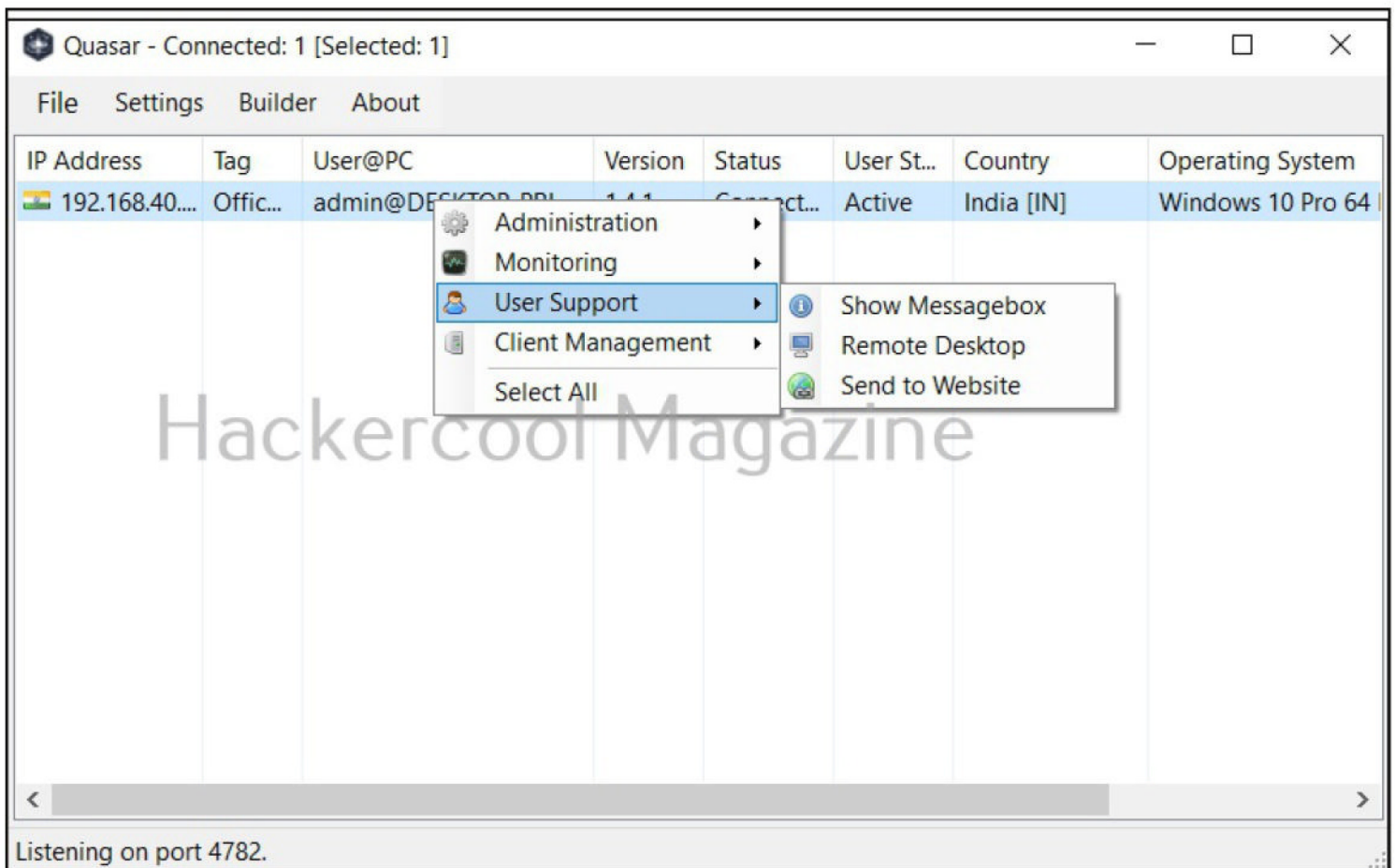
Magzter

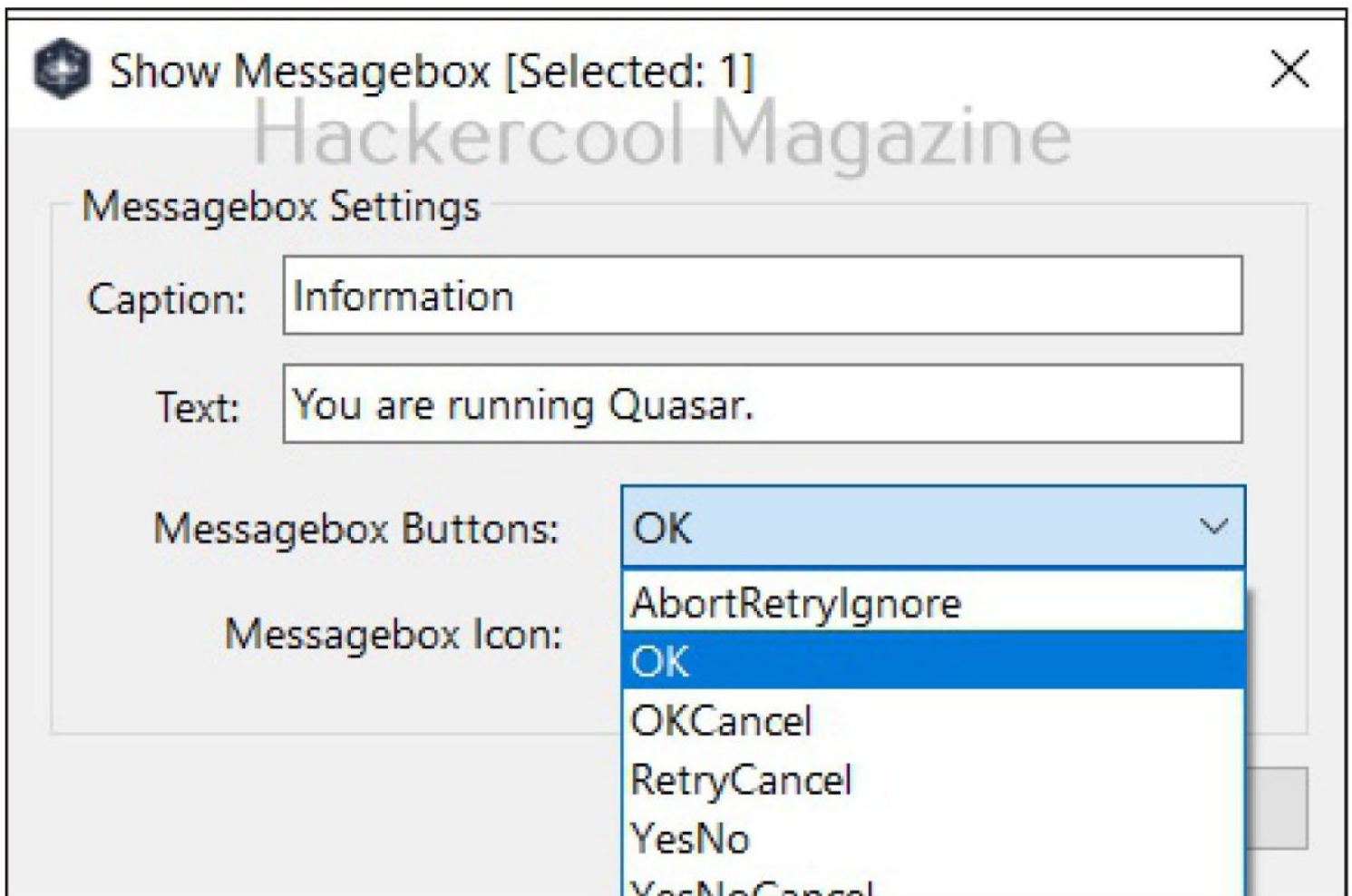
Quasar Client
 Remote desktop session started
 Quasar Client

Not just viewing, we can even enable the mouse and keyboard option on Remote Desktop and do whatever we want. For example, let's change the Google query a bit.



From the “show message box” function of Quasar RAT we can make a message box popup on the target system.





We can also make the browser on the target system to open a webpage or website we want using the “send to website” function.

Visit Website [Selected: 1]

URL:

☒ Visit hidden (recommended)

Visit Website

Visit Website [Selected: 1]

URL:

☒ Visit hidden (recommended)

Visit Website

← → ↻ 🔒 https://www.hackercoolmagazine.com ☆ 📄 📷 📁 ☰

**HACKERCOOL**
Simplifying Cybersecurity

Home

12 Free eBooks

Subscription

Products

Login

₹0 0 items



Blog

Contact us ▼

Chat with us 



https://www.hackercoolmagazine.com

Search

The “client management” menu of Quasar RAT contains settings related to the RAT itself and its connections. Using this, you can update reconnect, disconnect and even uninstall the Quasar client from the target system.

Kali Linux 2024.3

WHAT'S NEW

The makers of Kali Linux have released another version of Kali Linux. Kali Linux is one of the most widely used penetration testing distros. Let's see what's new in the latest release of this widely popular hacking operating system.



Latest Features to be excited about

New tools

This latest release of Kali Linux is more about package updates than adding any new things. Even then the makers added 11 new tools to the latest release. Let's see what they are what they are used for in hacking. The first tool you should be excited about is "gsocket". This is a tool that allows two machines located in two different networks to communicate with each other.

With Python 3.12, you will no longer be able to use pip to download and install packages.

```
(kali㉿kali)-[~]  
$ gsocket  
ERROR: No program specified  
gsocket [-k file] [-s password] <programm> <parameters>  
-s <secret> Secret (e.g. password).  
-k <file> Read Secret from file.  
-p <ports> Range of listening ports to redirect [default=all]  
-T Use TOR.  
  
Example:  
$ gsocket -s MySecret /usr/bin/sshd -d  
# Server  
$ gsocket -s MySecret ssh root@gsocket  
# Client  
  
See 'gs-netcat -h' for more options.
```

Another tool that has been added to the arsenal is “hekatomb”. This tool extracts and decrypts all credentials from all domain computers.


```
(kali@kali)-[~]  
$ hekatomb
```

Hackercool Magazine



Because Domain Admin rights are not enough.
Hack them all.

Hackercool Magazine

@Processus

v1.5

```
usage: hekatomb [-h] [-hashes LMHASH:NTHASH]
               [-pvk PVK] [-dns DNS]
               [-port [port]] [-smb2]
               [-just-user JUST_USER]
               [-just-computer JUST_COMPUTER]
               [-md5] [-csv] [-debug]
               [-debugmax]
               target
```

Script used to automate domain computers and

Goshs is a server used to host payloads on a web server. It is just like simple HTTP server in Kali that we used so many times, but it is written in Go.

```
(kali@kali)-[~]
$ goshs
INFO [2024-10-07 07:45:50] Download embedded file
at: /example.txt?embedded
INFO [2024-10-07 07:45:50] Serving on interface l
o bound to 127.0.0.1:8000
INFO [2024-10-07 07:45:50] Serving on interface e
th0 bound to 192.168.249.172:8000
INFO [2024-10-07 07:45:50] Serving HTTP from /hom
e/kali
```

Another tool added is “graudit”. This tool is a simple script and signature sets using which you can find potential security flaws in source code of programs.

```
(kali㉿kali)-[~]  
$ graudit
```

Hackercool Magazine

```

      . _ _ _
      | _/_/_/ |
      / _ \ ` _ \ | | v _ | | \ \ _
 \ // / > | \// _ \ | / / / | | || |
 \ _ / | _ | ( _ / _ \ _ | | _ || _
 / _ _ /          v          v

```

grep rough audit - static analysis to

OPTIONS

-d <dbname> database to use or /path/to/file.db (uses default if not specified)

-A scan unwanted and difficult (ALL) files

-x exclude these files (comma separated list: -x *.js,*.sql)

-i case in-sensitive scan

-c <num> number of lines of context to display, default is 2

-B supress banner

-L vim friendly lines

-b colour blind friendly template

-z supress colors

-Z high contrast colors

-l lists databases available

-v prints version number

Another tool 'mxcheck' is used for security scanning of email servers.


```
(kali㉿kali)-[~]  
$ mxcheck -h
```

Hackercool Magazine

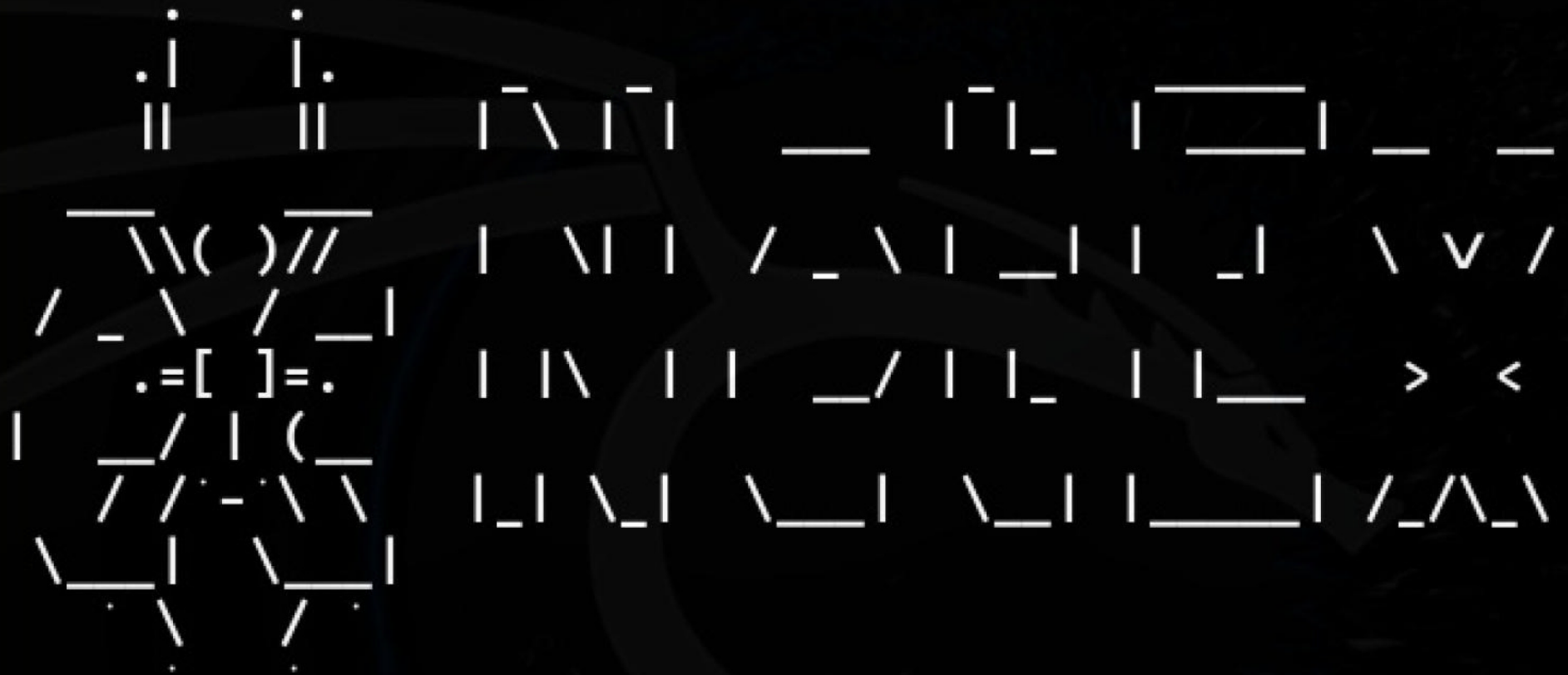
Usage of mxcheck:

-b, --blacklist	Check if the service is on blacklists
-S, --dkim-selector string	The DKIM selector. If set a DKIM check is performed on the provided service domain
-d, --dnsserver string	The dns server to be requested (default "8.8.8.8")
-f, --mailfrom string	Set the mailFrom address (default "info@foo.wtf")
-t, --mailto string	Set the mailTo address (default "info@baz.wtf")
-n, --no-prompt	Answer yes to all questions

Netexecute is a tool used for network service exploitation that helps automatically assessing the security of large networks.

```
(kali㉿kali)-[~]
$ netexec
[*] First time use detected
[*] Creating home directory structure
[*] Creating missing folder logs
[*] Creating missing folder modules
[*] Creating missing folder protocols
[*] Creating missing folder workspaces
[*] Creating missing folder obfuscated_scripts
[*] Creating missing folder screenshots
[*] Creating default workspace
[*] Initializing SMB protocol database
[*] Initializing FTP protocol database
[*] Initializing RDP protocol database
[*] Initializing SSH protocol database
[*] Initializing WMI protocol database
[*] Initializing WINRM protocol database
[*] Initializing MSSQL protocol database

[*] Copying default configuration file
usage: netexec [-h] [-t THREADS]
               [--timeout TIMEOUT]
               [--jitter INTERVAL] [--verbose]
               [--debug] [--no-progress]
               [--log LOG] [-6]
               [--dns-server DNS_SERVER]
               [--dns-tcp]
               [--dns-timeout DNS_TIMEOUT]
               [--version]
               {smb,ftp,rdp,ssh,wmi,winrm,mssql,vnc
,ldap}
               ...
```



Hackercool Magazine

The network execution tool

Maintained as an open source project by @NeffIs

Back, @MJHallenbeck, @_zblurx

A new variant of an Android banking trojan named TrickMo has been detected with features to steal a device's unlock pattern or PIN. This can enable the trojan to operate even when the device is locked.

Netscanner is a network scanning tool that has features like listing hardware interfaces, wifi scanning etc.

```
(kali㉿kali)-[~]
$ sudo netscanner
```

File Actions Edit View Help

Network Scanner (v0.5.3)

WiFi Networks					Interfaces			
time	ssid	ch	mac	sign	name	mac	ipv4	ipv6
show graph								

(1)Discovery (2)Packets (3)Ports

0/256 ip | Discovery

ip	m	192.168.249.0/24	hostn	vend
scan input/ESC				

export data | select

Sippts is a tool that can be used to audit VOIP server and devices using the SIP Protocol.

Bohemia and Cannabia, which are known as the world's largest and longest-running dark web market for illegal goods, drugs, and cybercrime services have been taken down by the Dutch police recently.


```
(kali㉿kali)-[~]
```

```
$ sippts
```

```
usage: sippts [-h]
```

```
                {video,scan,exten,rcrack,send,wssend,
enumerate,leak,ping,invite,dump,dcrack,flood,sniff,
spoofer,pcapdump,rtpbleed,rtcpbleed,rtpbleedflood,rtp
bleedinject}
```



SIPPTS version 4.0.12 (last version 4.1.1)

```
| LI LI LI | | |
```

CVE version 0.1 (updated)

```
| LI LI LI | | | 0o
```

://github.com/Pepelux/sippts

```
| LI LI LI | | | `0o
```

https://twitter.com/pepeluxx

```
| LI LI LI | | | 0o
```

```
| | | | | 0o
```

```
| .——. / \ | o0
```

```
| | | \ / | 0o
```

https

by Pepelux -

OpenAI announced that it has disrupted more than 20 operations and deceptive networks across the world that attempted to use its platform for malicious purposes since the start of the year.

```
-= SIPPTS is a set of tools for auditing VoIP systems based on the SIP protocol -=
```

Commands:

```
{video,scan,exten,rcrack,send,wssend,enumerate,leak,ping,invite,dump,dcrack,flood,sniff,spoof,pcapdump,rtpbleed,rtcpbleed,rtpbleedflood,rtpbleedinject}
```

video	Animated help
scan	Fast SIP scanner
exten	Search SIP extensions of a PBX
rcrack	Remote password cracker
send	Send a customized message
wssend	Send a customized message over WS

SQLMC stands for SQL Injection Massive hacker. This too is used to scan a domain for SQL injection vulnerability. It does this by scanning the given URL upto a specified depth, checks all the links for SSL injection vulnerability and reports it finds.

```
(kali㉿kali)-[~]  
$ sqlmc
```

Hackercool Magazine

A 5x10 grid of black and white line segments. The segments are arranged in a way that they form a stylized, abstract pattern. The pattern consists of various line segments, including horizontal, vertical, and diagonal lines, which are interconnected to create a complex, geometric design. The overall effect is a dense, black and white composition that resembles a stylized letter or a decorative element.

Version: 1.1.0

Author: Miguel Álvarez

```
usage: sqlmc [-h] -u URL -d DEPTH [-o OUTPUT]
```

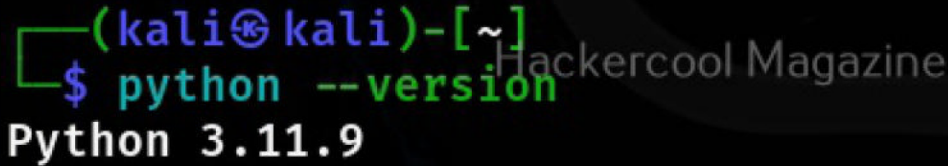
```
sqlmc: error: the following arguments are required:
```

-u/--url, -d/--depth

At the beginning of the article we told you this release is more about package updates that form the backend. They may not mean much to users but it's the backend that keeps the frontend working smoothly. At present, many in Kali are being transitioned. The first among this is GCC (GNU Compiler Collection). It is an open-source collection of compilers from the open-source GNU project that can be used to compile many programming languages like C, C++, Objective C, Objective C++, Fortran, Ada, D, Go and Rust.

The makers of this tool released a new version of this tool called GCC 14 in May 2024. Although new releases are not a new thing for any tool, this release made lot of changes, added support to new CPUs etc that are not present in previous versions of this tool. So, Kali is making transition to GCC 14.

But the important transition the makers of Kali are making is to Python 3.12.



```
(kali@kali)-[~]
$ python --version
Python 3.11.9
```

The latest version of the Python will remove some long deprecated apis, that is definitely going to break some packages. The transition is almost finished and the next release of Kali will have Python 3.12. Once this happens, the most important change you will notice while using Python 3.12 is that you no longer will be able to use PiP to download packages anymore. You have to use apt for that.

Other important updates added.

Two new mirrors have been added and another two mirrors are making a comeback which are going to make downloading Kali easy for users around the world. These 4 new mirrors use in Bulgaria, Italy, Netherland, South Korean.

Other features added.

Kali NetHunter has not been released yet and held back but they have added support to new devices. These are devices with Qualcomm Snapdragon SDM such as One Plus 6 (enchilada)/6T, SHIFT SHIFT 6mq (axolotus), Xiaomi Poco phone F1, Xiaomi MIX 25 (Polaris), Fair phone 4 etc.

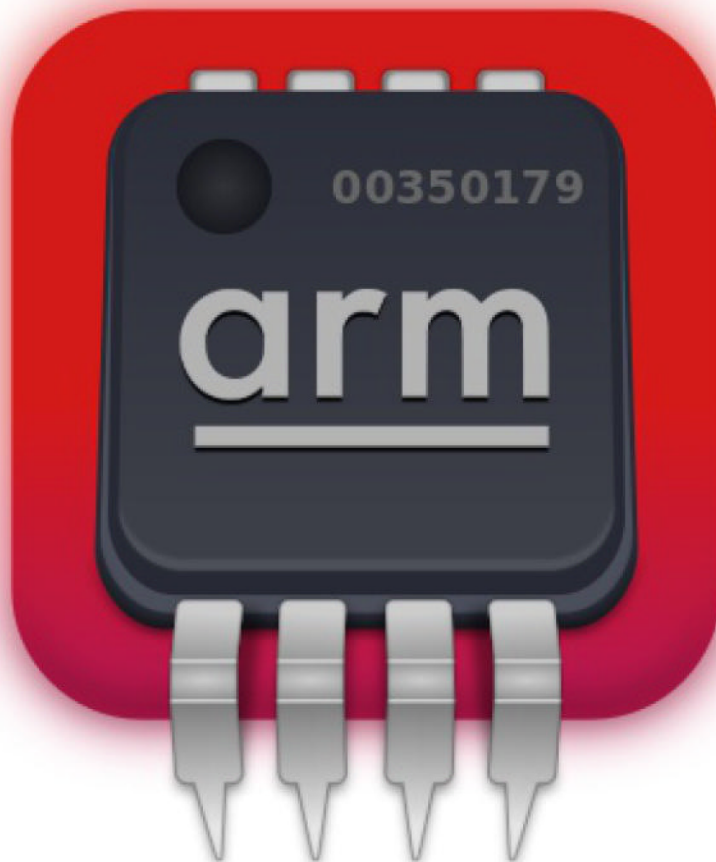
Mozilla, recently revealed that a critical security flaw impacting Firefox and Firefox Extended Support Release (ESR) is being exploited in the wild. It has urged its users to update the browsers to the latest update.

Hackercool Magazine



Similarly, the ARM version has also got some updates. The Raspberry Pi 4 kernel version has been upgraded to Raspberry Pi 6. Tell us your favorite update.

Hackercool Magazine



CrowdStrike: the massive companies you have never heard of with a hidden grip on our lives.

CYBER SECURITY

John Bryson

Professor of Enterprise and Competitiveness,
University of Birmingham

The world is saturated by services and products provided by companies that have a “secret grip” on the way we live. In 1951, the French-born American industrial designer Raymond Loewy described a typical day “of the average guy” from the moment he wakes up until he goes to bed. The point being that the average guy’s life was saturated with designed products.

In 2024, the average person may be woken by an alarm on a smartphone, and benefit from hot water that is controlled by smart heating controls – also linked to a smartphone and the internet. There might be a delivery tracked via the internet and a ring on a doorbell also linked to the internet. Online banking links them to an array of financial services.

Our lives are increasingly dependent on being able to access what I have termed the “cyber-energy-production plexus”. This “plexus” is basically an interwoven combination of elements that form a structure or a system. Regulating our modern lives, it needs to be “on” every second of the day.

It has formed around the multiple connections between telecommunications, energy, and manufacturing and service systems. It exposes everyone to unknown risks, including the sudden failure of the plexus and all the services coupled to it.

On July 19 2024, part of this plexus failed when the faulty CrowdStrike software update caused an outage, and the outcome was a minor digital pandemic across the world as the computer systems of whole industries came to a halt.

Consumers and producers began to appreciate how dependent they had become on interlinked technologies. The next digital pandemic could b

ring down the complete plexus for a few hours or even days.

Hidden grip

Perhaps unsurprisingly, the internet is at the centre of this plexus. There are more than 1,000 companies like CrowdStrike, whose actions can negatively impact on its functioning.

This of course includes the obvious names – Microsoft, Alphabet (Google, Google Cloud), Amazon, and Meta (Facebook). There are also less well-known companies like Cloudflare, which provides cloud cybersecurity services and domain name system services. Any disruption to Cloudflare results in problems accessing the cloud and disruption to the internet.

Then there are companies like Lumen Technologies, the US telecoms company that plays a critical role in global network connections. Lumen Technologies operates a tier one network. Tier one networks are the “motorways of the internet” as they provide high-capacity critical global links.

There are around 14 tier one networks. Any disruption of them would result in the fragmentation of the internet into smaller isolated networks that would be disconnected from one another.

Without the tier one networks, tier two networks would be left to provide service support – and these operate only regionally or nationally.

The list also includes companies like Swift, which facilitates cross-border payments. More than 11,000 financial institutions are connected to Swift, and this company plays a central role in the global financial ecosystem.

Any disruption to Swift could spark chaos, with problems transferring money around the world or some financial institutions experiencing dupli-

(Cont'd On Next Page)

cation of payment transfers.

Then there are telecommunications companies, such as Verizon, Rogers or BT. Both Verizon (2019) and Rogers (2022) have been involved in localised internet outages of short duration. Rogers, the Canadian telecommunications company, updated its network in 2022 and the outcome was a one-day outage that impacted on the country's critical infrastructure – debit payments, banking services and even hospitals and emergency service calls.

The plexus is configured around satellites and around 1.5 million kilometres of submarine fibre-optic cables that connect continents but which people are largely unaware of. Something like a natural disaster could damage these cables at any time, causing a catastrophic failure.

And there is a symbiotic relationship between the plexus and energy generation. Power failure could be a result of a fault with the plexus, which itself cannot operate without power.

The complexity of the plexus means that it is vulnerable to human error, as appears to have been the case in the CrowdStrike event. Then there are equipment failures and maintenance issues. Bad weather can also impact its operation, causing localised outages.

On top of all this it could be vulnerable to various types of cyberattacks, such as malware or border gateway protocol hijacking. In addition, tier one network cables are critical global infrastructure and can be damaged accidentally or targeted by terrorists or hostile military forces.

For people, companies and governments the key is to have contingencies in place to be prepared for failures and outages. But most of us are unprepared.

Any long-term disruption to the plexus would make everyday living exceedingly difficult, with the potential for looting and disturbances if, for example, internet-connected alarms were hit.

In the most severe cases – thankfully not seen in the CrowdStrike incident but tragically present in the case of internet outages in Sudan when emergency food supplies were disrupted – plexus failures can even cause death.

All this suggests that while there are undeniable advantages from the evolution of the cyber-energy-production-plexus, there remain a great many known and unknown risks.

This Article first appeared in The Conversation

SonicWall Firewall CVE-2024-40766

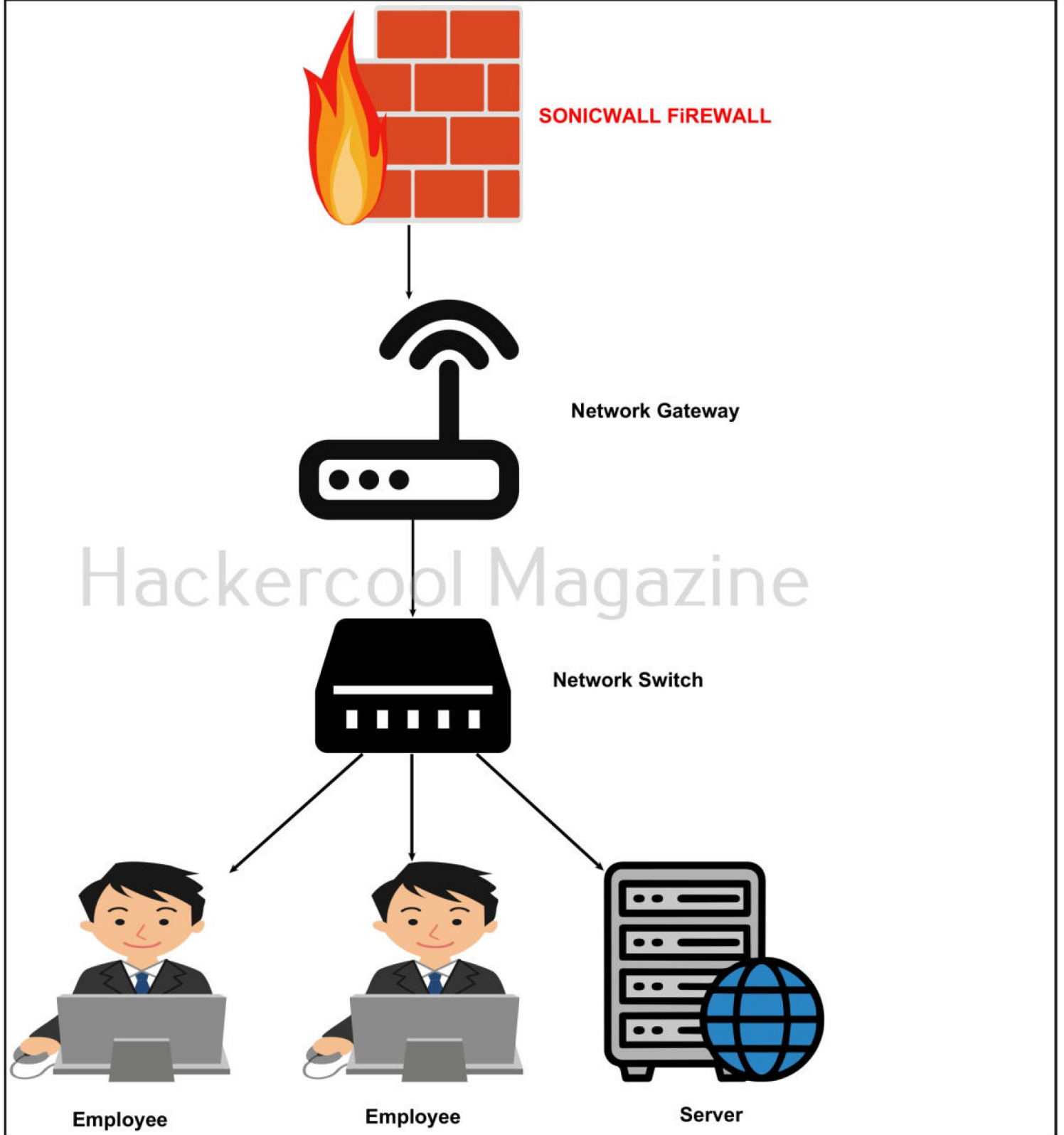
VULNERABILITY FOR BEGINNERS

SonicWall Firewalls are both hardware and virtual firewalls which are products of a American cyber security company named SonicWall. Many reputed companies and organizations use these firewalls.

SonicWall vulnerability CVE-2024-40766 is being actively exploited by the Akira ransomware group.

SONICWALL[®]

Like any typical firewall, they are placed between external and internal networks in large scale enterprises.



What is the vulnerability?

The vulnerability, being tracked as CVE-2024-0766 affects SonicOS, the operating system running on SonicWall's physical and virtual firewalls. SonicWall Gen 5, Gen 6, and Gen 7 devices running SonicOS upto 7.0.1-5035 are affected by this vulnerability.

The vulnerability is a critical improper access control vulnerability that allows attackers to gain admin access and control over SonicWall firewalls. After gaining administrator access on the SonicWall devices, the attacker can compromise security policies, deploy malware payloads or ransomware and even disable protections.



How this vulnerability can be exploited?

Although Firewalls are placed between WAN and LAN network, attackers can only exploit this vulnerability If WAN management of the firewall is enabled from the public internet or if SSLVPN is enabled on the firewall.

“By far, the greatest danger of Artificial Intelligence is that people conclude too early that they understand it.”

—Eliezer Yudkowsky

Hacker



Step 1:
Hacker scans for vulnerable
SonicWall Firewalls and
exploits them to gain access.

Internet



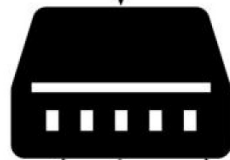
Sonicwall Firewall



Network Gateway



Network Switch



Employee



Employee



Server

Impact

The vulnerability which is already being exploited by threat actors in real-world can have drastic impact on the organisation if exploited. Apart from giving initial access on the network to hackers, this vulnerability can also allow attackers to deploy malware and ransomware. In fact, it is assumed that threat actors are deploying ransomware after exploiting this vulnerability.

Ransomware can encrypt the entire data on the target environment causing severe loss and damage.

How its exploitation can be prevented?

The vulnerable devices can be patched by updating to the latest release of the SonicOS operating system. Exploitation can also be prevented by restricting access to SonicWall Firewalls from trusted sources only. If WAN management of the firewall and SSLVPN is limited to trusted sources, there is less chance of vulnerability being exploited.

If WAN management is not needed, it can be disabled from public internet. Since the vulnerability is known to be already exploited from internet, it could be good if all users' passwords are reset and also enabling multi-factor authentication.

Exploding pagers and walkie-talkies are a reminder of how easily your devices can be hacked - here's how to make sure they are safe.

ONLINE SECURITY

Nick Hajli

AI Strategist and Professor of Digital Strategy,
Loughborough University

The recent attacks on walkie-talkies and pagers in Lebanon have highlighted the hidden vulnerabilities in everyday technology. These incidents underscore the need for individuals to understand the potential risks associated with their devices and to take proactive steps to protect themselves in an increasingly digital world where safety can be compromised.

Research shows that many people have significant concerns about security and privacy as technology advances. Statistics reveal an alarming rise in cyber threats and privacy breaches, underscoring the urgency of addressing these issues.

According to IBM, the average cost of a data breach worldwide reached US\$4.88 million (£3.65 million) in 2024, demonstrating the severe consequences of technological vulnerabilities.

So, are our smartphones and devices truly safe? With numerous reports of data breaches and privacy violations linked to technological development – especially concerning artificial intelligence (AI) – the recent attacks in Lebanon raise new concerns about the security of technology in an era where AI introduces complex challenges.

The pressing question for consumers is whether any of our devices can genuinely be deemed safe. If Israel can launch such an attack (and it has not confirmed it was behind the device attacks – but neither has it denied widespread reports insisting it was) other states may very well follow suit.

The Lebanon device attacks should serve as a crucial wake-up call regarding the vulnerabilities in devices we often take for granted. Part of the challenge lies in the less discussed impact of AI, which can track, analyse, and act on information in ways that pose risks to privacy and security, while AI brings substantial benefits to society, it a

(Cont'd On Next Page)

Also creates complex challenges, particularly in terms of democratic integrity and personal safety.

As technology increasingly becomes an indispensable part of our everyday lives – through smartphones, tablets, and smart home devices – it's really important to understand the risks associated with our dependency on this tech. There are some practical steps that we can all take to enhance our security and take control of our digital lives.

What you can do

1. Be careful who you buy from: One critical lesson is to be mindful of where you purchase your products. As technology advances, consumers often turn to price comparison apps to find cheaper options. But these less expensive products frequently originate from distant countries with complex supply chains. For example, in 2020, it was revealed that some Huawei and ZTE devices used in telecom infrastructure contained back doors, which led to allegations of espionage and resulted in some countries banning or limiting their use.

It's worth thoroughly researching the manufacturer before making a purchase. Before buying, check reviews and security certifications, and find out if the company has a history of security breaches or privacy concerns. Ensuring the manufacturer is reputable adds an extra layer of protection.

2. Understand potential risks: Older devices, such as pagers, often lack modern security features such as regular updates, making them more vulnerable to interception. Additionally, recent advances in AI raise concerns about the security of newer devices. For instance, AI algorithms used in smart home devices can learn user patterns and behaviours.

If these devices are compromised, hackers could use this information to orchestrate targeted attacks or gain unauthorised access to homes. It's crucial to assess the risks associated with both old and new technologies – and if you think them unsafe, it's best to just not use them.

3. Update devices regularly: Ensure you reg

ularly update your software and firmware to benefit from the latest security patches. Stick to devices that are still supported by their manufacturers, as unsupported devices may stop receiving vital security updates, leaving them vulnerable.

4. Keep your eyes on your tech: Anyone who is able to gain physical access to your device could tamper with it. Always store your devices securely when not in use, minimising the risk of unauthorised access.

5. Stay informed on cybersecurity issues: Keep yourself updated on the latest cybersecurity threats and learn how attackers exploit various technologies. Familiarise yourself with basic defensive practices, such as using strong, unique passwords and enabling two-factor authentication. Remember that many modern devices are interconnected, making them potential gateways for attacks. For example, a compromised smartphone could potentially infect your laptop or other devices on the same network.

Exercise caution with smart devices such as speakers, cameras, and wearables by ensuring they are properly configured, using encrypted connections, and limiting unnecessary data sharing.

By taking these steps, you can enhance your security and navigate the complexities of our technology-driven world with greater confidence.

**This
Article
first
appeared
in
The
Conversation**

DOWNLOADS

[Kali Linux 2024.3](#)

<https://github.com/trailofbits/fickling>

[Quasar RAT](#)

<https://github.com/quasar/Quasar>

USEFUL RESOURCES

[Check whether your email is a part of any data breach](#)

<https://haveibeenpwned.com>

[Vulnera](#)

<https://github.com/hackercoolmagz/vulnera>

Follow Hackercool Magazine for latest updates



